



Institución Universitaria

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

EDGAR ALBERTO ACEVEDOARANGO

y

ADRIANA MARÍA ECHEVERRI LONDOÑO

INSTITUCIÓN UNIVERSITARIA I.T.M.

Medellín, Colombia.

2026

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

*Tesis de grado presentada como último requisito parcial
para optar al título de **Magister en Seguridad Informática**.*

Por:

EDGAR ALBERTO ACEVEDOARANGO

I.E. / M.B.A. / Esp. Negocios Internacionales / Esp. Ciberseguridad / Esp. Analítica de Datos

y

ADRIANA MARÍA ECHEVERRI LONDOÑO

I.Q. / M.B.A. / Esp. Gerencia de la Calidad / Esp. Ciberseguridad

Directores:

Francisco Eugenio López Giraldo. *PhD.*

Héctor Fernando Montoya Vargas. *M.S.T.I.C.*

Línea de Investigación: Ciencias Computacionales

Grupo de Investigación: Automática, Electrónica y Ciencias Computacionales

INSTITUCIÓN UNIVERSITARIA I.T.M.

Facultad de Ingeniería

Maestría en Seguridad Informática

Medellín, Antioquia, Colombia.

07 de abril de 2026.

Dedicatoria

Los autores dedican esta tesis de maestría, junto con todo su esfuerzo y aprendizaje, **A:**

Con todo el infinito amor, que solo es posible sentir, para todo aquel quién ama con incondicionalidad total, dedico este logro y todo el conocimiento adquirido durante este largo camino de esfuerzo académico, de aprendizaje, de investigación, de formación y de crecimiento personal y profesional, a mis adorados hijos, quienes son mi razón de ser y la inspiración de todos y cada uno de mis días, *Daniel Alberto Acevedoarango Echeverri* y *David Alejandro Acevedoarango Echeverri*.

Edgar Alberto Acevedoarango

Con todo el infinito amor, que solo es posible sentir, para todo aquel quién ama con incondicionalidad total, dedico este logro y todo el conocimiento adquirido durante este largo camino de esfuerzo académico, de aprendizaje, de investigación, de formación y de crecimiento personal y profesional, a mis adoradas sobrinas *María Paz Echeverri López* y *María Fernanda Echeverri Murillo* y a mis ahijados *Daniel Alberto Acevedoarango Echeverri* y *David Alejandro Acevedoarango Echeverri*.

Adriana María Echeverri Londoño

Medellín, 07 de abril de 2026.

Agradecimientos

Los autores expresan su sincero agradecimiento, por todo lo aprendido y la ayuda recibida, durante el largo camino de construcción de conocimiento recorrido para la consolidación del postgrado y de esta tesis de maestría en seguridad informática, **A:**

- Nuestros seres queridos por todo su aliento, paciencia, comprensión y apoyo incondicional durante este arduo camino de aprendizaje.
- **SERVIFLEX ARCO INTERNACIONAL S.A.S.** empresa patrocinadora, por su apoyo y soporte incondicional, sin el cual, no hubiera sido posible la formación de postgrado.
- **INSTITUCIÓN UNIVERSITARIA I.T.M.**, por su colaboración, apertura, flexibilidad, solidaridad, compromiso académico e investigativo, alta exigencia y excelencia académicas e investigativas.
- Todo el sector flexográfico y convertidor, de Colombia y de Latinoamérica, que participó en esta tesis de maestría, incluyendo empresas de banda angosta y empaques flexibles, compañías de banda angosta y etiquetas y al sector de cartón corrugado, nuestra gratitud a todos ellos, por su colaboración y aporte, en su calidad de fuentes primarias de información, fundamental e imprescindible, y de destinatarios finales de este esfuerzo de investigación aplicada que se deja con cariño como legado para nuestra querida industria. También, a todas las diferentes casas fabricantes internacionales que colaboraron en el desarrollo de esta tesis de maestría.
- Todos aquellos que, por involuntaria omisión y obligada brevedad, pero, que de alguna u otra manera, participaron en el sendero de este esfuerzo formativo de postgrado y que contribuyeron con esta causa.

A todos ellos, nuestra infinita gratitud por su incondicionalidad, voz de ánimo, generosidad, compromiso, aportes y contribuciones. Dios los bendiga siempre y les compense en felicidad, paz y armonía, toda su ayuda.

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

Medellín, 07 de abril de 2026.

Resumen

Esta tesis de maestría, titulada “*Diseño de un modelo de ciberseguridad la cadena productiva crítica de la industria flexográfica*”, responde a la necesidad de fortalecer la protección informática de la infraestructura TI de un sector esencial cuya producción se encuentra cada vez más digitalizada y automatizada. Este escenario ha incrementado los niveles de riesgo, exposición y vulnerabilidad frente a ciberataques, especialmente en las pequeñas y medianas empresas (PYMEs), que constituyen la mayor parte del sector y resultan altamente atractivas para los cibercriminales. Asimismo, estas organizaciones son susceptibles a otros tipos de incidentes como fallas técnicas, contingencias y desastres, lo que refuerza la urgencia de contar con un modelo de defensa cibernética sólido.

Con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, así como la continuidad y resiliencia operativa de la industria, esta investigación propone el diseño de un modelo de ciberseguridad basado en estándares internacionales, como la norma ISO/IEC 27001, el marco NIST 2.0 CSF y los CIS Controls, así como, también, en las buenas prácticas de seguridad informática para la infraestructura TI asociada con la gestión, control y operación de la infraestructura OT de la cadena de producción crítica de la industria flexográfica. El objetivo es ofrecer un enfoque adaptable, práctico, eficaz y económicamente viable para la protección sectorial de la infraestructura IT (tecnologías informáticas) asociada a la gestión y operación de los sistemas OT de la cadena de producción crítica de la industria flexográfica.

En este propósito, la estrategia metodológica desarrollada consistió en tres (3) fases principales: una primera etapa (fase 1) diagnóstico sectorial del estado y necesidades de la infraestructura TI respecto a seguridad informática mediante la aplicación de una encuesta, cuyo análisis permitió identificar vulnerabilidades, amenazas y realizar el respectivo análisis y evaluación del riesgo cibernético de los sistemas informáticos asociados a la cadena de producción; una segunda etapa (fase 2) de revisión y análisis

de referentes internacionales para seleccionar y definir los controles adecuados que permitieran consolidar un prototipo cibernético de defensa funcional, flexible, adaptable y práctico de los activos TI para las empresas; y, finalmente, una última y tercera etapa (fase 3) de validación y verificación del modelo de ciberdefensa digital para la infraestructura TI asociada a la cadena de producción crítica de la industria, asegurando su eficacia y efectividad en el contexto industrial real.

Un interesante aporte para resaltar de esta tesis de maestría, es la expansión, complementación, adaptación, mejoramiento y actualización del cubo de McCumber de la seguridad informática, un marco conceptual de ciberseguridad, presentado, en 1991, en la conferencia de la NCSC/NSA e ideado por John R. McCumber, al cual se aplicó un proceso ingenieril de innovación derivado de una necesidad técnica y metodológica colateral que surgió del proceso investigativo, y que estribó en transmitir de manera sencilla y entendible los conceptos técnicos de ciberseguridad al personal no especializado de las compañías. Al efecto, el nuevo marco “Cubo Campanito de la Ciberseguridad Industrial” (CCCI) se creó como nuevo marco técnico de ciberprotección y como una herramienta metodológica, pedagógica y didáctica que, combina la tradición técnica y teórica de la seguridad informática con un enfoque contemporáneo orientado al sector industrial y de PYMEs, lo cual constituye un valor agregado relevante dentro de los resultados y productos logrados en esta tesis de maestría en seguridad informática.

Palabras Claves:

Ataques informáticos, Cadena productiva, Ciberseguridad, Controles, Industria flexográfica, Infraestructura crítica, Pequeña y mediana industria (PYME), Riesgo informático.

Abstract

This master's thesis, entitled "Design of a cybersecurity model for the critical production chain of the flexographic industry" responds to the need to strengthen cybersecurity protection of the TI systems that supports various OT processes in an essential sector whose production is increasingly digitalized and automated. This scenario has increased the levels of risk, exposure, and vulnerability to cyberattacks, especially in small and medium-sized enterprises (SMEs), which constitute most of the sector and are highly attractive objectives to cybercriminals. Furthermore, these organizations are susceptible to other types of incidents such as technical failures, contingencies, and disasters, reinforcing the urgency of having a robust cyber defense model.

To ensure the confidentiality, integrity, and availability of information, as well as the continuity and operational resilience of the industry, this research proposes the design of a cybersecurity model based on international standards: ISO/IEC 27001, NIST 2.0 CSF framework, CIS Controls guidelines and cybersecurity best practices for the TI infrastructure associated with management of OT processes of the critical production chain of the flexographic industry. The objective is to offer an adaptable, practical, effective, and economically viable approach for the sector-specific protection of IT infrastructure associated with the management, control, and operation of the OT systems of the critical production chain without including the own OT infrastructure.

For this purpose, the methodological strategy developed consisted of three (3) main phases: a first stage (phase 1) diagnosis of the status and needs of sectoral computer security through the application of a survey, whose analysis allowed to identify vulnerabilities, threats and carry out the respective analysis and evaluation of cyber risk; a second stage (phase 2) of review and analysis of international references to select and define the appropriate controls that would allow consolidating a functional, flexible, adaptable and practical cyber defense prototype for companies; and, finally, a last and third

stage (phase 3) of validation and verification of the digital cyber defense model, ensuring its efficiency and effectiveness in the real industrial context.

An interesting contribution to highlight from this master's thesis is the expansion, complementation, adaptation, improvement and updating of the McCumber cube of computer security, a framework presented, in 1991, at the NCSC/NSA conference and devised by John R. McCumber, to which an engineering innovation process was applied derived from a collateral technical and methodological need, which arose from the research process, and which consisted of transmitting cybersecurity concepts to companies in a simple and understandable way. To this goal, the Industrial Cybersecurity Tinker Bell Cube (ICTBC) is a new cyber protection framework and methodological and pedagogical tool that combines the technical and theoretical tradition of computer security with a contemporary approach oriented to the industrial and SME sectors, which constitutes a relevant added value within the results and products of this research.

Keywords:

Controls, Critical infrastructure, Cyberattacks, Cybersecurity, Flexographic industry, Small & medium enterprises (SMEs), Production chain, IT risk, IT infrastructure.

Índice o tabla de contenido

	Pág.
Dedicatoria	VII
Agradecimientos	VIII
Resumen	IX
Abstract	XI
Índice o tabla de contenido	XIV
Lista de figuras	17
Lista de tablas	19
Lista de anexos	21
Lista de siglas	23
1. Introducción	27
1.1 Diseño de un modelo de ciberseguridad para la infraestructura TI asociada a la cadena productiva crítica de la industria flexográfica	28
1.2 Pregunta de investigación	29
1.3 Objetivos	29
1.3.1 Objetivo general.....	29
1.3.2 Objetivos específicos	29
1.4 Alcance y delimitación	30
1.5 Contexto y antecedentes	30
1.6 Planteamiento del problema	34
1.7 Justificación e importancia del problema	35
1.8 Dimensión e impacto del problema.....	37
1.8.1. Ciberseguridad y ciberataques en la industria real.....	41
1.8.2. Ciberseguridad y ciberataques en el sector flexográfico.....	44
2. Marco teórico y estado del arte	46
2.1 Marco teórico	46

2.1.1	Técnica de impresión e industria flexográfica	47
2.1.2	Industria, infraestructura TI y seguridad informática	52
2.2	Estado del arte	68
3.	Metodología.....	73
3.1	Metodología de investigación.....	74
3.1.1	Enfoque y tipo de investigación	74
3.1.2	Fases de la investigación	52
3.2	Marco lógico	76
3.3	Desarrollo del marco lógico	78
4.	Resultados	81
4.1	Resultados de la fase 1 respecto al diagnóstico del estado, necesidades y requerimientos de seguridad de la infraestructura TI asociada a la cadena de producción de de la industria flexográfica.....	81
4.1.1	Resultados de la actividad 1.1 de la fase 1	82
4.1.2	Resultados de la actividad 1.2 de la fase 1	91
4.2	Resultados de la fase 2 respecto a la revisión de los estándares y referentes internacionales y las buenas prácticas de seguridad informática y consolidación del diseño del modelo de ciberseguridad	109
4.2.1	Resultados de la actividad 2.1 de la fase 2	111
4.2.2	Resultados de la actividad 2.2 de la fase 2	111
4.3	Resultados de la fase 3 respecto a la verificación y validación del modelo de ciberseguridad para la industria flexográfica.....	131
4.3.1	Resultados de las actividades de la fase 3.....	131
4.3.2	Nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI).....	147
5.	Discusión y análisis de resultados	155
6.	Consideraciones finales.....	155
5.1	Conclusiones	155
5.2	Recomendaciones	158
5.3	Lecciones aprendidas	160
5.4	Trabajos futuros.....	164
	Bibliografía y referencias	171
	Anexos	176

Lista de figuras

	Pág.
Fig. 1. Tipos de ciberataques comunes a empresas y PYMEs. 2024.....	41
Fig. 2. Tendencias en ciberataques en sectores de infraestructura crítica en Latinoamérica, 2024.....	43
Fig. 3. Tendencias globales de ciberataques por tipo de industria en 2024.....	44
Fig. 4. Web sites corporativos de una empresa del sector flexográfico.	57
Fig. 5. Prevención en seguridad informática, analogía con sector salud.	62
Fig. 6. Infraestructura de producción de una empresa esencial del sector flexográfico ..	64
Fig. 7. Fases metodológicas aplicadas para el desarrollo y solución de esta tesis de maestría.	75
Fig. 8. Estructura metodológica de investigación aplicada para el desarrollo de esta tesis de maestría.	80
Fig. 9. Gráfico de resultados por pregunta obtenidos en diagnóstico de estado y requerimientos de seguridad de la información en sector flexográfico 2025.	86
Fig. 10. Análisis de Pareto de los aspectos críticos de ciberseguridad obtenidos en la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico.	89
Fig. 11. Procedimiento de consolidación del resultado obtenido del análisis y la evaluación del riesgo cibernético para la infraestructura TI asociada a la cadena productiva crítica sectorial.....	92

Fig. 12. Mapa de calor inicial del riesgo informático en la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica..	103
Fig. 13. Modelo de ciberseguridad para la infraestructura informática asociada a la gestión de los procesos OT de la cadena crítica del sector flexográfico.	112
Fig. 14. Modelo de ciberseguridad para la infraestructura TI asociada a la gestión de la cadena de producción crítica de la industria flexográfica. Desglose completo con actividades.....	123
Fig. 15. Diagrama de flujo para aplicación práctica del modelo de ciberseguridad.	128
Fig. 16. Análisis de Pareto de los resultados obtenidos en la validación del modelo de ciberseguridad desarrollado para los sistemas TI vinculados a la gestión de la cadena de producción crítica de la industria flexográfica.....	139
Fig. 17. Reducción significativa de riesgos cibernéticos obtenida con la consideración de modelo de ciberseguridad para los sistemas TI de la industria flexográfica y confirmada mediante la respectiva prueba conceptual de validación.....	142
Fig. 18. Mapa de calor final obtenido con la consideración del modelo de ciberseguridad asociados a la gestión de los procesos OT de la cadena de producción crítica de la industria flexográfica	143
Fig. 19. Representación tridimensional completada del nuevo marco Cubo Campanito de Ciberseguridad Industria (CCCI). Versión completa	148

Lista de tablas

	Pág.
Tabla 1. Marco lógico.....	76
Tabla 2. Marco muestral de aplicación del instrumento metodológico de diagnóstico inicial.....	82
Tabla 3. Encuesta de diagnóstico de estado y necesidades de seguridad de la información del sector flexográfico. Resumen.	84
Tabla 4. Tabulación de resultados de encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico (2025).	85
Tabla 5. Matriz DOFA elaborada con base en los resultados de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025.	90
Tabla 6. Escalas de valoración de la criticidad del riesgo (Fase 1. Actividad 1.2).	96
Tabla 7. Escalas de valoración, probabilidad, impacto, gravedad y aceptabilidad del riesgo informático.....	101
Tabla 8. Resultados obtenidos de análisis y la evaluación del riesgo en la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica.....	102
Tabla 9. Alternativas u opciones de tratamiento del riesgo informático.	103

Tabla 10. Mapa de aceptabilidad inicial del riesgo cibernético para la infraestructura TI analizada.....	105
Tabla 11. Convenciones de la matriz de riesgos y mapa de calor de la infraestructura TI analizada.	107
Tabla 12. Riesgos identificados en la infraestructura TI asociada a la cadena de producción del sector flexográfico como resultado de la elaboración del análisis y evaluación del riesgo informático en la industria flexográfica en 2025 (matriz de riesgo y mapa de calor).	109
Tabla 13. Resumen del análisis de la mitigación de riesgos cibernéticos identificados en la infraestructura TI asociada a la cadena de producción de la industria flexográfica con el modelo de ciberseguridad propuesto	131
Tabla 14. Resumen de la encuesta de validación realizada para la verificación del modelo de ciberseguridad desarrollado para la industria flexográfica.	135
Tabla 15. Escala de Likert para la encuesta de verificación del prototipo cibernético protectivo desarrollado para la industria flexográfica.....	137
Tabla 16. Resultados de la validación del modelo de ciberseguridad desarrollado	135

Lista de anexos

	Pág.
Anexos	178

Anexo Nro. 1. Diagnóstico del estado actual y necesidades de la seguridad de la información del sector flexográfico.

Anexo Nro. 2 Tabulación de resultados de encuesta de diagnóstico del estado actual y necesidades de la seguridad de la información en el sector flexográfico.

Anexo Nro. 3. Autodiagnósticos obtenidos de los resultados de la encuesta de diagnóstico sectorial flexográfico (Autoevaluaciones según norma ISO 27001 y marco NIST 2.0 CSF).

Anexo Nro. 4. Matriz de riesgo informático y mapa de calor - Análisis y evaluación del riesgo cibernético actual del sector flexográfico.

Anexo Nro. 5. Controles seleccionados de la revisión de estándares internacionales y buenas prácticas de seguridad informática para el sector flexográfico.

Anexo Nro. 6. Modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Anexo Nro. 7. Validación del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Anexo Nro. 8. Tabulación y análisis de resultados de la encuesta de validación final del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Anexo Nro. 9. Autodiagnósticos finales obtenidos de los resultados de la encuesta de verificación del modelo de ciberseguridad (Autoevaluaciones según norma ISO 27001 y marco NIST 2.0 CSF).

Anexo Nro. 10. Matriz de riesgo informático y mapa de calor finales - Análisis y evaluación del riesgo cibernético final basada en los resultados obtenidos de la prueba de concepto (encuesta de verificación) realizada para validación del modelo de ciberseguridad.

Anexo Nro. 11. Nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI). New Industrial Cybersecurity Tinker Bell Cube (ICTBC) framework

Anexo Nro. 12. Estructura metodológica de investigación que condujo a la creación del nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI).

Anexo Nro. 13. Productos de esta tesis de maestría en seguridad informática. Artículos publicados, o confirmados y a publicar, en revistas indexadas.

Anexo 14. Productos de esta tesis de maestría en seguridad informática Participaciones, cursos y eventos. Certificaciones obtenidas en eventos, cursos y capacitaciones realizados durante y para el desarrollo de esta investigación de tesis de maestría en seguridad informática.

Lista de siglas

A continuación, se consigna el listado en orden alfabético de las siglas utilizadas en esta tesis de maestría en seguridad informática, a saber:

19CCC: Decimo Noveno Congreso Colombiano de Computación (Cajicá, 2025)

AI: Inteligencia Artificial (Artificial Intelligence).

ANDIGRAF: Asociación de la Industria Gráfica de Colombia.

APT: Amenaza Persistente Avanzada (Advanced Persistent Threat).

AWS: Servicios Web de Amazon Corporation (Amazon Web Services).

BCM: Unidad de volumen de cada una de las microceldas de un anilox.

BCP: Plan de Continuidad (Business Continuity Plan).

CCCI: Cubo Campanito de Ciberseguridad Industrial.

CEPAL: Comisión Económica para América Latina y el Caribe.

CIS: Centro de Seguridad del Internet (Center for Internet Security).

CIS Controls: Marco de pautas de mejores prácticas para la seguridad informática desarrollado por el Centro de Seguridad del Internet (Center for Internet Security).

COBIT: Objetivos de Control para la Información y Tecnologías Relacionadas (Control Objectives for Information and Related Technology) de la ISACA.

CSIRT: Equipo de respuesta a incidentes de seguridad informática (Computing Security Incident Response Team).

DDoS: Ataque de Denegación de Servicio Distribuido (Distributed Denial of Service).

DRP: Plan de Recuperación de Desastres (Disaster Recovery Plan).

EDR: Sistema de detección y respuesta ante amenazas de dispositivos de punto final (Endpoint Detection and Response).

ERP: Sistema Integral de Gestión Empresarial diseñado para modelar y automatizar la mayoría de los procesos de negocio como finanzas, logística, recursos humanos, etc. (Enterprise Resource Planning).

ICS: El Sistema de Control Industrial es la combinación de hardware y software diseñada para controlar procesos industriales y que representa el núcleo operativo que permite la automatización de los procesos físicos. (Industrial Control Systems).

ICTBC: Industrial Cybersecurity Tinker Bell Cube (ver el Anexo Nro. 11).

ICS: Sistemas Operativos de Control Industrial (Industrial Control Systems).

IEEE: Instituto de Ingenieros Eléctricos y Electrónicos (Institute of Electrical and Electronics Engineers).

INCIBE: Instituto de Ciberseguridad de España.

IoT: Internet de las Cosas (Internet of Things).

IT: Tecnologías de la información.

IRP: Plan de manejo y gestión de incidentes (Incident Response Plan).

ISAAC: Sistema Inteligente de Supervisión y Control Avanzado de Tiempo Real del Sistema Eléctrico Nacional

ISC2: Consorcio de Certificación Internacional en Seguridad de Sistemas de Información (International Information System Security Certification Consortium).

ISO (ISO/IEC): Organización Internacional de Normalización y Estandarización (International Organization for Standardization).

IT: Tecnologías de la Información (Information Technologies).

ITM: Instituto Tecnológico Metropolitano (Medellín, Colombia).

LPI: Lineatura Anilox en líneas (microceldas) por pulgada lineal.

EMS: Software encargado de controlar y supervisar en tiempo real lo que ocurre en la planta de producción (Manufacturing Execution System).

NSA: Agencia de Seguridad Nacional de los Estados Unidos de América (National Security Agency).

NICE: Iniciativa Nacional para la Educación en Ciberseguridad (National Initiative for Cybersecurity Education) de los Estados Unidos de América.

NIST 2.0 CSF: Marco de ciberseguridad versión 2.0 del Instituto Nacional de Estándares y Tecnología de los Estados Unidos de América. (National Institute of Standards and Technology of United States of America).

OEA: Organización de los Estados Americanos.

OT: Tecnologías de Operación u Operacionales (Operational Technologies).

PHVA: Planear, Hacer, Verificar y Actuar, fases del Ciclo de Deming o ciclo PHVA.

PMU: Unidades de medición fasorial (Phasorial Metric Units).

PYMEs: Sector de Pequeñas empresas, Medianas empresas y Microempresas.

ROA: Arquitectura orientada al riesgo. Es un enfoque de análisis y evaluación que integra la gestión del riesgo directamente en el diseño y la estructura de los sistemas de información y que considera el riesgo cibernético como un evento externo. (Risk Oriented Architecture).

RSAC: Conferencia internacional de ciberseguridad patrocinada por RSA Data Security, Inc. (RSA Conference).

RTO: Objetivo de Tiempo de Recuperación en el contexto de tiempos de recuperación de un sistema informático ante un ciberincidente.

RPO: Objetivo de Punto de Recuperación en el contexto de tiempos de recuperación de un sistema informático ante un ciberincidente.

SCD: Sistemas de Control Digital (Digital Control Systems – DCS).

SCo2: Sociedad Colombiana de Computación.

SGSI: Sistema de Gestión de Seguridad de la Información.

SNMyD25: Simposio Nacional de Maestrías y Doctorados 2025.

TIC: Tecnologías de la Información y la Comunicación.

USAF: Fuerza Aérea de los Estados Unidos de América (United State Air Force).

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

1.Introducción

1.1 Diseño de un modelo de ciberseguridad para la infraestructura TI asociada a la cadena productiva crítica de la industria flexográfica

La ciberseguridad se ha convertido en un pilar fundamental para la protección de las organizaciones modernas, especialmente en sectores industriales cuya operación y negocio dependen de sistemas informáticos y activos digitales que operan cadenas de producción críticas. La industria flexográfica, como parte esencial de la cadena productiva de la economía real, enfrenta, actualmente, panorama complejo marcado por la digitalización, la automatización y el consecuente incremento de su superficie de exposición a ciberamenazas. En particular, según se infiere de [1] y [2], las pequeñas y medianas empresas (PYMEs) presentan limitaciones estructurales, como restricciones presupuestales, carencia de personal especializado y aplicación insuficiente de controles de seguridad, que las hacen más vulnerables ante acciones maliciosas y ciberataques, como, también, ante la ocurrencia de fallas tecnológicas, contingencias técnicas, calamidades o desastres.

Este contexto plantea la necesidad urgente de desarrollar modelos de protección que sean eficaces, prácticos y económicamente viables, y en este curso de acción, la presente tesis

de maestría presenta el diseño de un modelo de ciberseguridad para la infraestructura TI que soporta diferentes procesos de OT dentro de la industria flexográfica que, fundamentado en estándares internacionales y buenas prácticas de seguridad informática, se adapta a la realidad operativa de la industria actual y, en particular, de las PYMEs del sector flexográfico. En este orden de ideas, el propósito investigativo último de esta tesis de maestría es contribuir con la consolidación de un modelo de ciberseguridad que, permita ayudar con la protección y el aseguramiento de la confidencialidad, integridad y disponibilidad de la seguridad de la información de los sistemas TI e infraestructura computacional e informática que soportan la cadena de producción crítica de la industria flexográfica y que contribuya con la continuidad operativa y la resiliencia organizacional a nivel sectorial. A dichos efectos, esta tesis de maestría en seguridad informática tiene los siguientes propósitos, a saber:

1.2 Pregunta de investigación

Esta tesis de maestría gira alrededor de la búsqueda de una solución práctica a la siguiente pregunta de investigación, que obra como guía de toda la metodología de investigación utilizada para la consolidación del modelo de ciberseguridad propuesto y que se presenta más adelante, a saber:

- *¿Mediante qué modelo de ciberseguridad, basado en estándares internacionales y buenas prácticas de seguridad cibernética, se podría conservar la confidencialidad, integridad y disponibilidad de la infraestructura TI y demás sistemas computacionales e informáticos asociados a la gestión de los sistemas OT de los procesos productivos críticos de una PYME del sector flexográfico?*

De esta manera, la pregunta de investigación establecida es una guía sólida para el desarrollo de esta tesis de maestría en seguridad informática, pues, delimita claramente el problema central que se enfoca en proteger los sistemas informáticos asociados a la gestión de la cadena de producción crítica de una PYME o empresa del sector flexográfico

y orienta en la búsqueda de una solución fundamentada en estándares internacionales ampliamente aceptados y reconocidos, como la norma ISO 27001, el marco NIST 2.0 CSF y los CIS Controls. En este punto vale mencionar que la infraestructura OT, por razones de alcance metodológico queda suscrita a un trabajo futuro. Además, al enfatizar en los tres (3) pilares de la seguridad (confidencialidad, integridad y disponibilidad), invita a un análisis integral que no solo aborde la implementación técnica, sino, también, la gestión de riesgos informáticos, las políticas de seguridad organizacionales y la cultura de la ciberseguridad.

1.3 Objetivos

Esta tesis de maestría en seguridad informática tiene los siguientes objetivos, a saber:

1.3.1 Objetivo general

“Proponer el diseño de un modelo de ciberseguridad, basado en estándares internacionales y buenas prácticas de seguridad, que permita la conservación de la confidencialidad, integridad y disponibilidad de los sistemas informáticos asociados a los procesos productivos críticos de una PYME del sector flexográfico”.

1.3.2 Objetivos específicos

1.3.2.1 Diagnostico sectorial y evaluación de riesgo

“Identificar el estado actual, las necesidades y requerimientos de seguridad de la información de los procesos y de la cadena de producción crítica de una PYME de la industria flexográfica”.

1.3.2.2 Revisión de estándares internacionales y consolidación del prototipo de ciberseguridad

“Caracterizar los elementos aplicables de los estándares internacionales seleccionados y de las buenas prácticas de seguridad informática mediante la consolidación del diseño del modelo de ciberseguridad propuesto”.

1.3.2.3 Verificación del modelo de ciberseguridad

“Validar el modelo de ciberseguridad mediante una prueba de concepto”.

1.4 Alcance y delimitación

Es importante resaltar que el dominio esta tesis de maestría, en concordancia con lo expresado en el objetivo general está delimitado a los sistemas informáticos, es decir, que esta exclusivamente circunscrito a la infraestructura TI asociada a la cadena productiva crítica del sector flexográfico, sin incluir la tecnología OT. A este respecto, es importante hacer notar que el establecimiento de esta línea de delimitación metodológica ciñe el alcance del modelo de ciberseguridad propuesto exclusivamente al dominio de la infraestructura de las tecnologías de la información que soportan la gestión estratégica, administrativa y logística de la cadena productiva crítica en la industria flexográfica.

Dentro del alcance relacionado con los activos de la infraestructura TI, se incluyen hardware (equipos físicos), software (programas y aplicaciones), talento humano (personal) e información (bases de datos et al), y, por tal razón, el prototipo cibernético protectivo propuesto incluye la defensa y aseguramiento de redes corporativas, servidores de datos, aplicativos y programas de gestión empresarial, sistemas de respaldo de información, servicios en la nube, terminales de usuario final, programas, personal operativo y de la organización, et al.

En este contexto, el alcance metodológico establecido no incluye propiamente la tecnología OT (*sistemas de control industrial, SCADAS, PLC, sensores, actuadores, etc.*), parte igualmente fundamental, pero, que se ha de tratar debidamente en un trabajo futuro. Así, el modelo de ciberseguridad desarrollado solo se realizó para abarcar el diseño de controles para los sistemas computacionales e informáticos, por los cuales se permite el acceso y uso de los sistemas OT y por los que fluyen las primeras capas de datos desde un ambiente externo.

De otra parte, bajo esta misma premisa y, también, por razones del alcance metodológico establecido, se excluyeron los sistemas Enterprise Resource Planning (ERP) y el Manufacturing Execution System (EMS), puesto que, fundamentalmente, su ubicación estratégica se localiza dentro de la arquitectura industrial, ya que actúan como nodos de convergencia que vinculan la operación y la ejecución técnica en planta con la gestión empresarial de naturaleza administrativa. Al situarse en la frontera de las operaciones industriales (sistemas OT) su aseguramiento requiere de protocolos de disponibilidad en tiempo real y consideraciones de seguridad funcional que no forman parte del marco técnico de un modelo centrado estrictamente en la infraestructura informática (sistemas TI) establecida.

De esta forma el alcance y la delimitación establecida metodológicamente, reconocen la existencia de la parte OT, del control industrial y de su punto de convergencia entre TI y OT para el intercambio de datos de la cadena de producción, pero, por la delimitación expuesta, se dejan para un trabajo de investigación futura y las acciones de protección se limitan estrictamente a la capa informática y a los activos y sistemas TI.

Así pues, trabajos futuros de investigación han de desarrollar formalmente y en detalle, la parte de las tecnologías OT, incluyendo la protección de toda la infraestructura de control industrial y demás sistemas operacionales, para completar un modelo de ciberseguridad integral, del cual el alcance metodológico de esta tesis de maestría en seguridad informática presenta solo uno de sus componentes, pues se busca, exclusivamente asegurar y proteger la infraestructura TI asociada a la cadena productiva crítica del sector flexográfico.

1.5 Contexto y antecedentes

La pasada pandemia de Covid-19 destacó la importancia estratégica de la industria flexográfica como un pilar insustituible de la economía real, cuya producción de empaques y etiquetas resulta vital para el sostenimiento de sectores críticos como el alimentario y el farmacéutico. No obstante, el sector enfrenta desafíos de seguridad informática crecientes debido a la digitalización y automatización de sus procesos, lo que ha incrementado la exposición de los sistemas de gestión y operación ante ciberataques sofisticados y fallas técnicas en su infraestructura TI. Esta vulnerabilidad es particularmente crítica en las pequeñas y medianas empresas (PYMEs) que, además de constituir la mayoría del sector según se afirma en [1], operan frecuentemente con recursos limitados y carecen de capacidades técnicas especializadas, lo que las convierte en objetivos altamente atractivos para los ciberatacantes de acuerdo con lo expuesto en [2].

Esta problemática se ve agravada por la carencia de modelos de ciberseguridad adecuados y adaptados a las capacidades de estas organizaciones, un vacío que genera gran preocupación sectorial debido al riesgo de que un ataque a los sistemas TI pueda interrumpir de forma temporal, o definitiva, la operación de las líneas de producción afectando a toda la organización e impactando el sector. Ante esta urgencia, la presente tesis de maestría tiene como objetivo fundamental presentar el diseño de un modelo de ciberseguridad integral para la infraestructura y los sistemas informáticos y computacionales de gestión, operación y control de la cadena productiva en las PYMEs y empresas del sector flexográfico. Al efecto, el fundamento principal serán los estándares internacionales ya mencionados y las buenas prácticas de seguridad informática, las cuales han sido totalmente adaptadas al estado actual, las necesidades de la industria y las restricciones operativas que caracterizan a las PYMEs y empresas del sector.

El modelo de ciberseguridad planteado, se presentara posteriormente y busca contribuir y mejorar la protección de la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura y los sistemas computacionales e informáticos asociados a la gestión de dichos procesos productivos de naturaleza crítica e

irremplazable, así como, también, propender por el aseguramiento de la robustez operacional y de la resiliencia digital organizacional de las PYMEs y empresas del sector flexográfico, cuya importancia y criticidad fue demostrada por la pasada pandemia de Covid-19 de 2020.

Para cumplir con este propósito, la investigación se estructuró en una metodología compuesta por tres (3) fases que inició con la evaluación del estado actual y las necesidades de seguridad de los sistemas TI del sector, seguida de una etapa de análisis e integración de estándares internacionales, como la ISO 27001 [3], el marco NIST 2.0 CSF y los CIS Controls [5], permitiendo así la definición de un conjunto de controles que consolidaron el prototipo de defensa para la infraestructura TI presentado en esta tesis.

Dicho modelo fue validado en una etapa final mediante una prueba de concepto consistente en una encuesta de verificación bajo los mismos lineamientos del diagnóstico inicial a efectos de realizar un comparativo que permitiese estimar la mitigación del riesgo cibernético. Como resultado, el modelo ofrece una solución práctica, económica y escalable que permite a las PYMEs y empresas flexográficas (e incluso a organizaciones con cadenas productivas críticas similares) afrontar riesgos informáticos con mayor eficacia y efectividad, protegiendo sus activos críticos mientras se fomenta una sólida cultura de ciberseguridad respaldada por el compromiso directivo para fortalecer la resiliencia digital en todo el entorno industrial analizado.

El modelo de ciberseguridad planteado en esta tesis integra controles técnicos, administrativos y de diversa índole, extraídos de los estándares internacionales y buenas prácticas ya mencionados, para conformar una estrategia defensiva preventiva y proactiva que supervise continuamente los procesos informáticos de la infraestructura TI vinculada a la producción. Este prototipo busca establecer políticas de seguridad eficaces y flexibles que se adapten a la realidad de las PYMEs flexográficas, incorporando programas permanentes de capacitación para el personal operativo, quienes, a pesar de ser esenciales, suelen ser relegados en las estrategias organizacionales de ciberseguridad. Adicionalmente, el enfoque integral garantiza no solo medidas preventivas, sino también capacidades de detección y respuesta rápida que minimizan el impacto de incidentes, en los sistemas TI, orientando la gestión de la cadena de producción hacia la persistencia y la resiliencia operacional en el entorno informático del sector.

La validación del modelo se realizó mediante una prueba de concepto consistente en una encuesta de verificación aplicada a las mismas empresas flexográficas inicialmente indagadas, con el fin de comparar la eficacia y efectividad del prototipo frente la mitigación del riesgo cibernético en los sistemas TI respecto a los resultados obtenidos en el diagnóstico sectorial inicial. Este análisis comparativo permitió estimar el grado de mitigación del riesgo y evaluar la pertinencia de las soluciones diseñadas, confirmando que el modelo ofrece una protección robusta alineada con los referentes internacionales. De este modo, se aseguró que el prototipo cibernético protectivo no solo cumpliera con los estándares técnicos, sino que, adicionalmente, fuera una solución aplicable y realista para el entorno de las PYMEs de la industria en estudio.

Así pues, se espera que los resultados de este esfuerzo investigativo y de aprendizaje, consolidados en esta tesis de maestría, no solo brinden una solución flexible, adaptada y práctica a las necesidades particulares de las PYMEs y empresas del sector, sino que, también, contribuyan al desarrollo de una cultura organizacional de ciberseguridad, promoviendo una visión preventiva y proactiva frente a los desafíos actuales que plantea, a la sociedad toda, a la economía y, en particular, a la industria, la digitalización acelerada y la conexión permanente al ciberespacio de los activos IT críticos.

1.6 Planteamiento del problema

La digitalización, la automatización, la robótica, el internet de las cosas (IoT), los sistemas de control digital (SCD) [6], y, más recientemente, la llegada de la inteligencia artificial (AI), han venido revolucionado la producción industrial y, en particular, las cadenas productivas de industrias esenciales como el sector de la flexografía. En efecto, según afirma [7], las líneas de producción de las empresas se están transformando, mutando del enfoque mecánico tradicional a un entorno altamente automatizado y digitalizado soportado en tecnologías de punta, donde la infraestructura productiva, incluidos, pero, no limitados a equipamiento y máquinas que están ya permanentemente conectadas a redes computacionales e informáticas y al ciberespacio y que son gestionados, controlados y operados a través de sistemas informáticos.

Esta nueva realidad ha permitido una mayor eficiencia y control en los procesos productivos, pero también, ha incrementado la superficie de exposición y la vulnerabilidad de la infraestructura productiva crítica de estas empresas ante ciberataques a sus sistemas computacionales. En especial, en el caso de las PYMEs, como se infiere de [1] y [2], se aprecian grandes retos de seguridad de la información, en los sistemas informáticos que gestionan sus procesos productivos, ya que muchas de ellas no cuentan con protocolos de ciberseguridad sólidos, ni mecanismos de continuidad operativa que les permitan mitigar riesgos asociados a ciberamenazas, fallas tecnológicas, contingencias técnicas, calamidades o desastres, que, eventualmente, puedan comprometer los sistemas informáticos asociados a sus cadenas de valor.

En este contexto, y tal como se desprende de la revisión del estado del arte y, en particular, como se recomienda en los trabajos de [8], [9], [10] y [11], este proyecto de tesis propone el diseño de un modelo de ciberseguridad para la infraestructura TI asociada a la cadena de producción crítica de PYMEs del sector flexográfico, basado en elementos aplicables derivados de los estándares internacionales ampliamente reconocidos y aceptados ya mencionados, que serán complementados por otros componentes adicionales extractados de las mejores prácticas en seguridad de la información [11].

En este sentido, el modelo a proponer buscará ofrecer una protección integral mínima, pero, efectiva, a los sistemas informáticos vinculados a los activos críticos de la cadena productiva de las PYMES del sector y a la información clave que soportan, en razón a que, particularmente, este tipo de empresas, por su tamaño y características, requieren un enfoque adaptable, personalizado, flexible y económico, que les permita implementar o fortalecer su seguridad cibernética, sin comprometer su sostenibilidad organizacional, ni tampoco, sus obligaciones normativas y legales, pero, sobre todo, asegurando su continuidad productiva y su resiliencia operativa digital.

1.7 Justificación e importancia del problema

La creciente digitalización de los procesos industriales que, según [6] inició con la infraestructura del sector eléctrico y, más recientemente, la interconexión al ciberespacio

de los sistemas informáticos ha expuesto a las cadenas productivas de las empresas, especialmente de las PYMEs, como afirma [2], a una amplia gama de amenazas cibernéticas en razón a su característica falta de recursos técnicos, financieros y humanos, dedicados u orientados a atender la seguridad informática corporativa. En efecto, la industria flexográfica, como sector clave e irremplazable de la economía global, regional y local, no es una excepción y cobra relevancia debido a su insustituibilidad como fuente de productos de las cadenas de suministro de otras industrias igualmente críticas para la sociedad. La vulnerabilidad de las cadenas productivas críticas del sector flexográfico representa un riesgo significativo para la continuidad operativa, la resiliencia productiva y la competitividad de las compañías del sector.

De otra parte, según [13], en un mundo cada vez más interconectado, la ciberseguridad se ha convertido en un pilar esencial para garantizar la sostenibilidad y la competitividad de las industrias y sectores de la economía real y, en particular, de sus PYMEs, del cual no es exento el sector industrial significativamente importante y crítico, como es el caso de la industria flexográfica que, a su vez, es fuente de productos para otras industrias y sectores catalogados formalmente como industrias e infraestructuras críticas, como el caso de la alimentaria, la farmacéutica, la de bienes y servicios de primera necesidad, entre muchas otras.

Al respecto, y según afirman [12] y [13], la digitalización y la automatización, impulsadas por tecnologías de la Industria 4.0, han transformado las cadenas de producción, exponiéndolas a riesgos cibernéticos significativos, razón por la cual, esta tesis de maestría propone soluciones útiles, necesarias y urgentes para el sector, a través de la consolidación del diseño de un modelo de ciberseguridad adaptado a la cadena productiva crítica de las PYMEs de dicha industria, abordando desafíos específicos de recursos limitados y altas exigencias operativas de cadenas de producción críticas para la sociedad y la economía y, si bien existen tentativas incipientes, medidas muy básicas, e implementaciones, en mayoría muy someras, de numerosos referentes marcos y estándares de seguridad de la información en muchas empresas, pocos de ellos están diseñados específicamente para las necesidades de las PYMES de un sector tan neurálgico como es el sector de la industria flexográfica.

La mayoría de las soluciones de ciberseguridad, seguridad informática o seguridad de la información existentes en las PYMEs del sector flexográfico, según afirma [14] y corroborado por los conceptos de [15] y [24], son básicas e incipientes, demasiado genéricas o muy elementales, siendo estas circunstancias, factores que motivan y justifican el diseño del modelo de ciberseguridad para la infraestructura TI que aquí se presenta, el cual ha de basarse en un análisis exhaustivo de las características particulares del sector industrial de la flexografía, identificando los principales riesgos cibernéticos a los que están expuestas sus compañías y, en particular de sus PYMEs, en aras de proponer un prototipo de ciberseguridad que consolide un conjunto de medidas de seguridad cibernética aplicables, prácticas y efectivas, de tal manera que se asegure la triada de la CIA en los sistemas informáticos asociados a la gestión y operación de sus cadenas productivas esenciales.

1.8 Dimensión e impacto del problema

La problemática de ciberseguridad que enfrenta actualmente, el sector real de la economía, en particular, la industria flexográfica no puede analizarse de forma unidimensional, pues, aunque los aspectos técnicos de la infraestructura TI (como la protección de sistemas, equipos, servidores, redes, aplicaciones, bases de datos y dispositivos conectados), constituyen el frente más visible del riesgo informático, realmente, no representan la totalidad del problema que, también, se extiende hasta los propios niveles organizacionales y a la infraestructura OT, que se mencionan para completar el contexto, pero, que, como ya se comentó anteriormente, por razones del alcance establecido, no son cubiertas por el prototipo cibernético protectivo desarrollado.

En este contexto real, la gestión de la seguridad informática implica una doble dimensión: una operativa-tecnológica, (recuérdese que el modelo de ciberseguridad esta desarrollado para la infraestructura TI y que la parte OT no está incluida y solo se menciona para contextualizar la situación) centrada en el aseguramiento de la infraestructura digital, y otra organizacional-estratégica, enfocada en los procesos de gobernanza, cultura de seguridad, concienciación y capacitación, cumplimiento normativo y toma de decisiones informadas. Esta condición dual, según [9], [12], [13], [14], [15] y [16], refuerza la necesidad

de proteger los sistemas informáticos y la infraestructura TI, considerando el entorno estratégico que los gobierna, lo cual, de no tenerse en cuenta, siempre conducirá a soluciones incompletas o ineficaces (al caso específico bajo estudio, este esfuerzo de investigación debe complementarse con la adecuada protección de la infraestructura OT).

Desde el punto de vista técnico, y tal como apunta [14] y se corrobora más adelante, de los resultados del diagnóstico sectorial del estado y necesidades de ciberseguridad de la infraestructura TI efectuado, la industria flexográfica depende de manera creciente de herramientas digitales para la gestión, el control y la operación de la cadena de producción crítica (aunque, también, para labores de supervisión y mantenimiento remoto de equipos desde la casa fabricante, actividades de diseño gráfico y preparación de la impresión, la gestión de pedidos, el matizado de tintas, la programación de producción, el almacenamiento, la logística, et al y que, como ya se ha mencionado, forman parte de los sistemas OT que deberán atenderse en un trabajo futuro para completar este desarrollo circunscrito a los sistemas TI.

Por esta razón, la exposición de estos sistemas ante amenazas cibernéticas (como ingeniería social, malware, ransomware, accesos no autorizados o errores humanos) compromete directamente la confidencialidad, integridad y disponibilidad de la operación de la seguridad de la información de los sistemas informáticos asociados a la gestión, operación y control de la cadena de producción, poniendo en riesgo la continuidad operacional y la resiliencia digital de los sistemas TI.

Sin embargo, tal como afirman [12], [13], [15] y [16], cuando las ciberamenazas no están acompañadas de un marco protector conformado por políticas claras, sensibilización y formación del personal, evaluación de riesgos periódica y estrategias definidas de continuidad y de resiliencia digital, los controles técnicos, por sí solos, no son suficientes para garantizar una defensa en profundidad, ni una protección efectiva, ni tampoco, una respuesta eficaz en la infraestructura TI. Por ello, se hace necesaria la integración de ambos planos, estratégico-administrativo y tecnológico, en cuanto a las tecnologías TI y por la delimitación de OT expuesta anteriormente, a efectos del diseño de cualquier modelo de ciberseguridad.

En consecuencia, como se desprende de [4] y recomienda [13], abordar integralmente la ciberseguridad en la industria flexográfica requiere articular la dimensión técnica con la dimensión estratégica, de manera coordinada, continua y contextualizada, pues, esta integración debe permitir no solo la implementación de tecnologías de defensa y monitoreo, sino, también, la definición de políticas internas robustas en el nivel organizacional, así como la asignación de roles y responsabilidades claras, el desarrollo de concientización y de capacidades humanas, y la inclusión de la ciberseguridad como parte de la cultura organizacional de las empresas. Así, se facilita el fortalecimiento de continuidad operativa y de la resiliencia frente a un entorno digital en permanente evolución, donde las ciberamenazas son cada vez más sofisticadas y adaptativas y, también, donde la velocidad de respuesta puede marcar la diferencia entre la continuidad de los sistemas TI que gestionan la producción o su interrupción o colapso.

Además, la situación se ve agravada por la brecha de ciberseguridad existente entre grandes industrias y PYMEs, pues, como se ha mencionado, estas últimas, que constituyen el núcleo mayoritario de la cadena productiva flexográfica, enfrentan limitaciones presupuestales, escasez de talento especializado y ausencia de modelos de gestión de la seguridad informática alineados con estándares internacionales ampliamente aceptados, como [3], [4], [5], y las normas [17], [18] e [19]. Esta realidad impide que muchas empresas adopten un enfoque proactivo de ciberseguridad y las condena a prácticas reactivas, incipientes e ineficaces, donde los incidentes cibernéticos se gestionan solo cuando ya han causado daño, es decir, cuando ya es tarde para las compañías.

En este contexto de potencial alto impacto, la adopción de marcos como la familia de normas ISO 27000 series [3], el NIST 2.0 CSF [4] y los CIS Controls [5], [17] e [18], aunados a un modelo de ciberseguridad funcional, adaptable y práctico, como el propuesto en [20] y [21], que está basado en el nuevo framework Cubo Campanito de la Ciberseguridad Industrial (CCCI), derivado, como valor agregado y con calidad de producto innovador resultado de esta tesis de maestría, son elementos esenciales para la solución del problema de ciberseguridad sectorial que, cada vez es más preocupante.

Así pues, como afirman [12], [13] y [15], concebir la ciberseguridad desde esta doble dimensión técnico-estratégica no solo optimiza los recursos disponibles y eleva la

eficiencia operativa, sino que permite consolidar una visión sostenible, escalable y resiliente de protección digital para el sector flexográfico. Ello contribuye directamente a la continuidad del negocio, a la confianza de los clientes y aliados, y a la sostenibilidad del ecosistema productivo frente a los retos de la transformación digital y las amenazas emergentes del ciberespacio.

De esta manera, esta tesis de maestría responde a una necesidad sentida y urgente de la industria flexográfica, enfocándose en la protección, la continuidad y la resiliencia operativas de las PYMEs del sector flexográfico frente a amenazas cibernéticas en un entorno productivo permanentemente interconectado y cada vez más interdependiente digital y cibernéticamente, por lo cual, consignados los aspectos anteriores, es importante anotar que, sobre el papel económico y el riesgo informático de las PYMEs en Latinoamérica, bien observan [1] que, este segmento productivo, representa el 99,5% de las empresas de la región y que, entre ellas, una gran mayoría son microempresas (88,4%).

De otro lado, como afirman [1] y a pesar de su innegable y mayoritario aporte económico, las PYMEs a menudo enfrentan desafíos significativos en cuanto a la gestión de la seguridad de la información, incluyendo y sin excepción de su cadena productiva esencial (considerada infraestructura crítica, como ya se mencionó, desde la pasada época de pandemia de Covid-19 en 2020) y, en particular, afrontan retos significativos respecto al manejo y la gestión del riesgo informático. Las PYMEs del sector flexográfico adolecen de la misma problemática y sus limitaciones económicas y de recursos presupuestales hacen de ellas aún más vulnerables y expuestas al riesgo informático y, consecuentemente, a los efectos e impactos del accionar mal intencionado de los cibercriminales.

En efecto, y especialmente, en el ámbito de la ciberseguridad, tal como aprecian [2], se reconoce el fenómeno como generalizado y necesario de atender, por lo cual, afirma que las PYMEs, al depender cada vez más de la tecnología para ser competitivas, están en riesgo de sufrir ciberataques que pueden causar pérdidas financieras y de reputación, por lo que la gestión de la seguridad informática y ciberseguridad se ha convertido en una necesidad primordial para su supervivencia y crecimiento. Esto debido a la creciente digitalización y la dependencia progresiva de la tecnología, como se infiere de [2], [7], [12]

y [13], ha ocasionado un incremento significativo de la superficie de exposición de las PYMEs y empresas del sector flexográfico ante diversos riesgos cibernéticos, a lo cual, también, deben incluirse los eventos fortuitos como fallas tecnológicas, contingencias, calamidades y/o desastres.

1.8.1. Ciberseguridad y ciberataques en la industria real

Como se observa, a continuación, en la Fig. 1, los ciberataques mediante técnicas como la suplantación con falsa identidad, las acciones maliciosas de insiders de las propias empresas y el ransomware están entre los vectores más significativos y a tomar en consideración por presentar niveles porcentuales altos (37%, 37% y 33%, respectivamente). No obstante, toda la distribución de los porcentajes de los diversos tipos de ciberataques (incluyendo suplantación de identidad o spoofing, amenazas internas, ransomware, malware, DDOS, phishing, APTs, etc.) recibidos por las empresas y, en concordancia con [2], [15], [24] y [25], conforman el preocupante escenario actual de abundantes dificultades y grandes riesgos que afectan a las industrias esenciales, independientemente de su objetivo, naturaleza, subsector y tamaño.

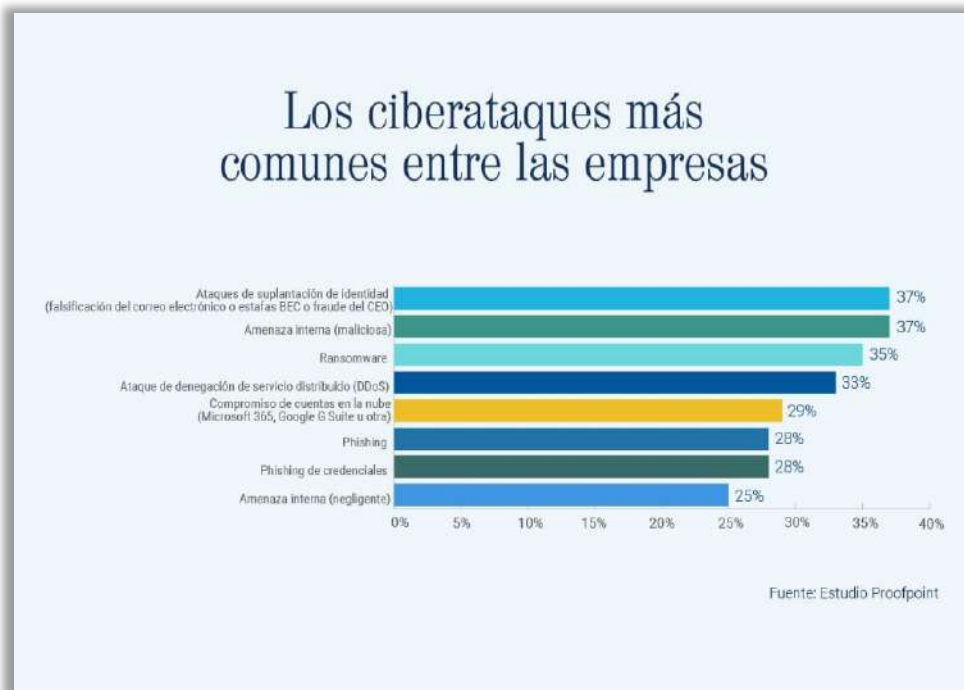


Fig. 1 Tipos de ciberataques comunes a empresas y PYMEs. 2024.
Nota. Tipos de ciberataques comunes a empresas y PYMEs. Fuente: tomado de [29].

Esta exposición al riesgo impacta tanto a grandes empresas como a PYMEs que, en especial, están normalmente restringidas por sus carencias de recursos económicos para inversión en soluciones tecnológicas, personal capacitado e implementación y desarrollo de protocolos formales de ciberseguridad, los cuales son elementos necesarios para enfrentar los tipos de amenazas informáticas y que, potencialmente, pueden poner en riesgo la infraestructura informática de gestión de la cadena productiva crítica de las empresas de un sector esencial como la flexografía.

De otra parte, y como se observa de los aportes de [1], de [7] y como se constata en la Fig. 1, el entorno de alta competencia y mercados globalizados, donde se depende del buen funcionamiento y operación ininterrumpida de las cadenas de producción de las empresas, ha llevado a que la masificación de las nuevas tecnologías y la permanente conexión al ciberespacio hayan ido transformando los procesos productivos en el ámbito industrial. Sin embargo, según [13], [22], [23] y [24], esta revolución tecnológica ha traído consigo una exposición creciente de la superficie de ataque de los sistemas informáticos y la aparición de ciberamenazas cada vez más frecuentes, sofisticadas y complejas, que ponen en riesgo las infraestructuras críticas de producción.

La urgencia de garantizar la supervivencia, continuidad operativa y resiliencia informática de los sistemas TI, en este nuevo contexto es innegable, sobre todo en un sector como el flexográfico, donde la digitalización ha expuesto las vulnerabilidades de sus cadenas productivas ante ciberataques o contingencias y fallas tecnológicas, según [2], [7], [27], [28] y [29]. Esta es una realidad que no solo incumbe al sector flexográfico, sino, también, a otros sectores industriales con características similares, razón por la cual, los resultados de esta investigación de tesis de maestría pueden ser útiles en otras industrias y entornos empresariales.

En efecto la justificación e importancia del problema bajo estudio estriban en la búsqueda de la corrección de falencias cibernéticas protectivas, proporcionado el diseño de un modelo de ciberseguridad que, bajo el imperio de estándares internacionales ampliamente aceptados y de buenas prácticas de seguridad, sea de fácil aplicación, practicidad, eficacia, efectividad y que solvente esta sentida necesidad sectorial y corporativa de protección de las infraestructuras de producción esenciales, dotando, o fortaleciendo, de capacidad de

resiliencia a los procesos operativos digitales de las empresas sectoriales, en especial a las PYMEs, como se aprecia en [28].

La Fig. 2 devela que, desde tiempos posteriores a la pandemia de Covid-19, toda Latinoamérica se ha tornado objeto de ciberataques, siendo naciones como Brasil y México, por su población y economía las más atacadas. Sin embargo, países como Colombia y Perú, proporcionalmente, no se quedan atrás y, en la actualidad, el volumen de ciberataques es cada vez más creciente, complejo y sofisticado, superando los 350.000 que se registra [29]. En la actualidad, la situación, como es de conocimiento público, es aún más grave, puesto que las ciberamenazas han venido creciendo a un ritmo exponencial, tanto en frecuencia, como en complejidad y sofisticación.



Fig. 2 Tendencias en ciberataques en sectores de infraestructura crítica en Latinoamérica, 2024.

Nota. Durante los últimos tres (3) años, los ciberataques han incrementado significativamente. Fuente: tomado de [32].

A este respecto, la Fig. 3, registrada por [32], muestra cómo se distribuyen, a nivel mundial y en 2024, diversos tipos de vectores de ataque cibernéticos sobre los diversos sectores de la sociedad, siendo educación, gobierno y salud los más afectados, pero, sin dejar atrás a las infraestructuras industriales. Vale la pena notar que, el sector más afectado es el educativo con 2.454 ciberataques por semana, mientras que el segmento industrial presenta 897 ciberataques por semana y esto pone de manifiesto como el riesgo por ataques cibernéticos continúa creciendo de manera acelerada, constituyendo un gran riesgo para las empresas e industrias.

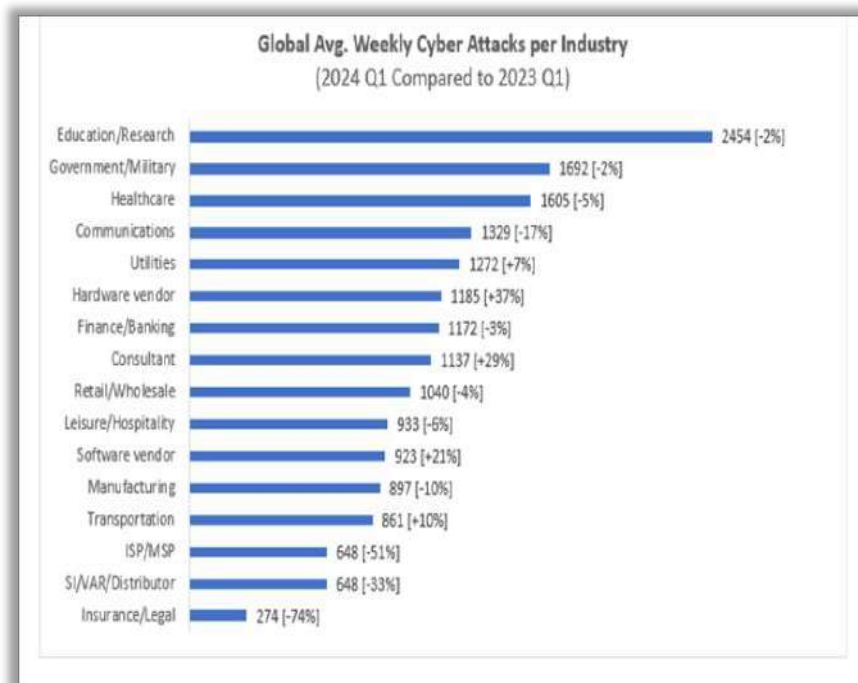


Fig. 3 Tendencias globales de ciberataques por tipo de industria en 2024.

Nota. Ciberataques globales a infraestructuras críticas industriales 2024. Fuente: tomado de [35].

Como se puede inferir, en particular para las PYMEs del sector flexográfico, no tener una defensa en profundidad y una estrategia proactiva sólidas que le permitan antelar, detectar, identificar, enfrentar, responder, mitigar, recuperar y superar incidentes cibernéticos maliciosos, como se infiere de [14] y [30] y [31] que concuerdan en que la criticidad de la situación de riesgo cibernético en las PYMEs, pues son un objetivo frecuente de ciberataques, y muchas no denuncian por temor a afectar su reputación y que muy a pesar de que un ciberataque podría llevar a la quiebra al 57% de ellas, estas no consideran la ciberseguridad como una prioridad, percibiéndola como compleja, costosa y que requiere altos conocimientos técnicos. Por ello, [32] afirma que el portal Check Point Research recomienda desarrollar un protocolo de ciberseguridad efectivo que atienda la necesidad de enfoques integrales y preventivos.

1.8.2. Ciberseguridad y ciberataques en el sector flexográfico

El sector de la industria flexográfica ha dejado de ser un objetivo invisible para convertirse en un blanco de interés para los ciberdelincuentes y grupos de ransomware. Entre 2020 y

2025, el panorama de amenazas evolucionó desde ataques genéricos hacia operaciones altamente dirigidas, aprovechando la creciente digitalización de las líneas de producción. Casos de alto impacto, como el ataque a la multinacional de empaques WestRock en 2021 [7], demostraron que un incidente en la infraestructura de impresión flexográfica puede paralizar cadenas de suministro completas, afectando la distribución de bienes de primera necesidad como alimentos y medicinas a nivel global.

Durante el periodo 2022-2024, la tendencia se desplazó hacia el "ataque por proximidad", donde empresas líderes como Multi-Color Corporation (MCC) [8], sufrieron interrupciones que evidenciaron la vulnerabilidad de la industria de etiquetas. Estos incidentes confirmaron que la flexografía no solo es vital para la logística, sino que actúa como un "vector puente" donde los atacantes comprometen al proveedor para escalar sus acciones hacia los sistemas de clientes corporativos de mayor envergadura, lo que subraya la importancia de la corresponsabilidad técnica y humana en la ciberseguridad.

Ya en 2025 y los primeros meses de 2026, el foco de los ataques se ha centrado con mayor intensidad en las PYMEs del sector. Al ser organizaciones que suelen operar con recursos limitados, han sido víctimas de grupos de ransomware que buscan pagos rápidos mediante la interrupción total de la línea de producción. Reportes recientes de firmas de ciberseguridad industrial publicados por Label & Narrow Web (LNW) [9], indican que el sector es ahora uno de los más golpeados, con incidentes que no solo buscan el secuestro de datos, sino la manipulación de los sistemas de control de gestión, lo que valida la urgencia de implementar modelos de defensa en profundidad.

Finalmente, como consigna [9] el riesgo en la industria flexográfica ha pasado de ser una posibilidad técnica a una crisis de continuidad operativa. El aumento de ataques registrados en países como Colombia, donde la manufactura lidera las estadísticas de incidentes, refuerza la necesidad de marcos como el CCCI que se presenta, más adelante, como valor agregado adicional de esta tesis. La evidencia muestra que sin una cultura de ciberseguridad que integre al personal de planta y sin una arquitectura resiliente, la digitalización de la industria flexográfica seguirá siendo su mayor vulnerabilidad ante un entorno de amenazas cada vez más sofisticado.

2. Marco teórico y estado del arte

2.1 Marco teórico

La industria flexográfica y sus diversos subsectores, como el de los empaques flexibles, las etiquetas y el cartón corrugado, según [10] y reconfirmado por el conocimiento y experiencia de los autores de esta tesis de maestría, desempeñan un papel fundamental en la economía real y como fuente insustituible de productos necesarios y esenciales para las cadenas de suministro de otras industrias similarmente críticas para la sociedad, razón por la cual cualquier interrupción, temporal o definitiva, de sus procesos productivos, dada la irremplazabilidad de su cadena de producción flexográfica, puede generar pérdidas económicas significativas, impactar los negocios, perturbar o dañar la credibilidad, la reputación, la imagen y la confidencialidad corporativas, pero, sobremanera, generar afectaciones importantes y daños irreparables a la economía nacional, a la calidad de vida de las personas y, en general, a la sociedad entera.

En este sentido, se debe entender que la flexografía es una industria fundamental por su capacidad para imprimir en materiales plásticos y ofrecer soluciones sostenibles para el empaque de productos de otras industrias esenciales, tal como afirma [17]. De similar forma, según [10], la industria flexográfica, ha venido experimentando una verdadera y significativa transformación tecnológica, principalmente en cuanto tiene que ver con la masificación de la digitalización y presencia de infraestructuras TI en los negocios, presente hoy día, en casi todos los sectores de la economía real, incluidas otras industrias, el comercio, los servicios, las comunicaciones, el entretenimiento, el transporte, entre otros muchos. En este punto y dicho lo anterior, es menester, reiterar que esta tesis está enfocada en las infraestructuras TI sin incluir sistemas OT.

Adicionalmente, y para el caso particular de las industrias productivas, la automatización

de las líneas o cadenas de producción ha venido intensificándose en los últimos tres o cuatro lustros como producto de la reconversión industrial y, en la actualidad, dichos procesos productivos, difícilmente sustituibles, como el caso de la impresión flexográfica, son gestionados, operados y controlados por medio de sistemas informáticos con permanente conexión al ciberespacio y, consecuentemente, expuestos ante eventuales ciberamenazas, fallas tecnológicas, contingencias, calamidades o desastres informáticos. Por esta razón y en aras de la transparencia y ética investigativa, es menester reconocer y resaltar la importancia de que, como trabajo futuro, la industria flexográfica ha de completar el presente prototipo de ciberseguridad, desarrollando la parte protectiva de sus sistemas OT.

2.1.1 Técnica de impresión e industria flexográfica

Como apuntan [10] y [17], la flexografía es una técnica de impresión actualmente muy usada en la industria. Grosso modo, la flexografía es un sistema de impresión rotativo de alta velocidad que utiliza planchas flexibles en relieve, antigua y tradicionalmente elaboradas en caucho y que, actualmente, se fabrican en materiales fotopoliméricos (polímeros sensibles a la luz), los cuales se usan para transferir tinta a viscosidad determinada sobre una amplia gama de sustratos, incluyendo papel, cartón, películas plásticas (films) y otros tipos de materiales de naturaleza metalizada (foil de aluminio, poliéster metalizado y otros).

Según afirma [10], la flexografía surgió a principios del siglo XX como una evolución rudimentaria del sistema de impresión anilina, en que se utilizaba dicho colorante para efectuar la impresión sobre el material. En efecto, como se infiere de [17], la flexografía fue inicialmente utilizada para imprimir empaques primarios de alimentos, pero, en sus inicios enfrentó críticas y resistencia por su baja calidad de reproducción. No obstante, con la incorporación de avances tecnológicos como las tintas de curado UV, el control digital del registro, los sistemas CTP (computer-to-plate) y el uso de anilox cerámicos de altísimas lineaturas (1000 a 2100 LPIs y más) grabados con tecnología láser de última generación, la flexografía ha alcanzado estándares de calidad de impresión comparables a otras técnicas de impresión industrial como el Offset o el Rotograbado (también denominado huecograbado).

En la actualidad, el sistema flexográfico industrial constituye la tecnología predominante en el sector productivo de empaques y, también, en la conversión y transformación de plásticos, pues, se trata de una tecnología que se adapta eficientemente a los requerimientos productivos de tirajes cortos, requisitos de diseño, necesidades de personalización, como se infiere de [10], [17] y [36]. Adicionalmente, la sostenibilidad y automatización en entornos industriales altamente competitivos, en los cuales la seguridad de la información, hoy día, es un asunto tan prioritario y esencial, como obligado de atender, al igual que otros ámbitos esenciales de la economía real. En razón a lo anterior, nuevamente, se reitera la importancia de completar este esfuerzo investigativo completando la protección cibernética de las infraestructuras OT.

En general, la industria flexografía está conformada por los siguientes sectores productivos, a saber:

- Empaques flexibles y banda ancha
- Etiquetas y banda angosta
- Cartón corrugado y otras aplicaciones industriales especiales (como laminación, estampación, recubrimiento, off set, etc.)

Este panorama industrial resalta la importancia de fortalecer las capacidades de seguridad informática sectoriales para los sistemas TI de la industria flexográfica, como se infiere de [2] y de las apreciaciones de [28], ya que, todos los días, muchas empresas, entre ellas las PYMEs, están adoptando tecnologías avanzadas con adquisiciones de líneas de producción nuevas o de segunda mano para sus infraestructuras productivas críticas, que incluyen tecnologías como la automatización, la robótica, el control digital, el internet de las cosas (IoT), el soporte de procesos con inteligencia artificial (AI) y Big Data, todas razones por las cuales, la infraestructura esencial de producción del sector flexográfico ya, hoy por hoy, es operada y controlada desde equipos informáticos y sistemas computacionales, es decir, a través de infraestructuras y sistemas de TI.

En efecto, esta infraestructura informática se encuentra mayoritariamente interconectada al ciberespacio de manera continua y permanentemente, lo cual, conlleva el aumento de la superficie de exposición de dichos sistemas informáticos asociados a la gestión de las cadenas productivas antes la abundancia y sofisticación de las amenazas informáticas, como bien afirman [15], [16], [18], [25] y [26] y, consecuente, también conlleva al aumento del nivel de riesgo cibernético.

De otra parte y como concuerdan [15], [16], [26] y [27], en este mismo contexto es oportuno hacer notar que un ciberataque a la cadena de producción crítica de una empresa flexográfica esencial puede tener consecuencias devastadoras, tanto para la propia organización, como para el suministro sectorial de productos derivados del sector, en especial, en el caso de las PYMEs. Entre los eventuales impactos indeseados se pueden incluir y mencionar los siguientes:

- Disrupción, suspensión o paralización de los procesos y de la cadena de producción (ocasionado por eventos en los sistemas TI y no causados por la infraestructura OT, que no se considera en esta tesis).
- Pérdida de información y datos confidenciales (clientes, proveedores, aliados estratégicos, propiedad intelectual, entre otros).
- Afectaciones en la cadena de suministros corporativa y daños a la reputación
- Pérdida de negocios, de clientes y de nuevas oportunidades con costos elevados asociados a lucro cesante
- Suspensión o cese definitivo de operaciones, pérdida de negocios, cobro de indemnizaciones de parte de clientes perjudicados, sanciones por incumplimiento del marco legal y normativo, particularmente, del tributario, entre muchas otras.
- Daños reputacionales y de imagen, siempre y cuando la gravedad del incidente no conduzca a condiciones cierre permanente o quiebra económica.
- Afectaciones a las cadenas de suministro esenciales de otras industrias críticas, como la alimentaria, farmacéutica, de bienes y productos de primera necesidad,

entre otras, donde los productos de la industria flexográfica forman parte insustituible e irremplazable.

De otra parte, vale mencionar en este punto que, como se reveló en Andigráfica 2025 [36], la industria flexográfica en Colombia tiene una notable relevancia y participación económica, tanto en el PIB nacional como en la economía real del país, derivada de las contribuciones conjuntas de los sectores de empaques flexibles, etiquetas y cartón corrugado. En efecto, según información gremial emanada de la Asociación de la Industria Gráfica de Colombia, ANDIGRAF [36], aproximadamente, unas quinientas ochenta (580) empresas operan en la industria del país, de las cuales ciento ochenta (180), aproximadamente, se dedican exclusivamente a la flexografía, específicamente en los segmentos de empaques, envases, etiquetas, embalajes y cajas, entre otros.

Esta contribución de la producción está conformada por una mayoritaria participación del segmento de las PYMEs, cuyo patrimonio societario oscila entre 855 millones de pesos y hasta 7.500 millones de pesos para el año de 2024. Según la misma fuente, estas actividades representan el 66,5% de los ingresos operacionales del sector en los últimos años, destacando la relevancia de las PYMEs en la industria nacional y en la economía del país.

Adicionalmente, vale comentar que, según [17], las empresas del sector flexográfico en Colombia tienen una concentración importante en regiones como Bogotá, Antioquia y el Valle del Cauca, debido a su infraestructura industrial y logística. Sin embargo, regiones como Atlántico, Bolívar, Risaralda y Santander, también, son centros industriales y, aunque no tan grandes, cuentan con algún tipo de presencia de empresas dedicadas a la flexografía. De otra parte, los polos urbanos son el asiento natural de la industria, destacándose ciudades como Bogotá, Medellín, Cali y Barranquilla, especialmente enfocadas en la producción de empaques flexibles, etiquetas y embalajes, cajas de cartón corrugado.

En este contexto, como afirman [2] y [17], la industria flexográfica, al igual que otras industrias y sectores de la economía real, enfrenta un escenario complejo y muy complicado de riesgo informático, debido a la llegada de la digitalización, la inteligencia

artificial (AI), el internet de las cosas (IoT), la automatización, la robótica, los sistemas de control digital (SCD) [6], la conectividad permanente al ciberespacio, la proliferación de redes inalámbricas, el trabajo remoto, entre otros muchos factores que, aumentan la superficie de exposición ante eventos cibernéticos maliciosos o, también, ante fallas técnicas, contingencias tecnológicas, calamidades o desastres.

Al respecto, y como lo expresa [37], los proveedores de servicios y productos esenciales tienen la obligación de implementar medidas gerenciales, financieras, administrativas, operativas y técnicas, para mejorar su ciberseguridad, pues el riesgo informático está siempre presente y se ha convertido, en un aspecto clave y prioritario para la gestión de la seguridad de la información en las organizaciones, a riesgo de sufrir impactos indeseados sobre los sistemas informáticos asociados a los procesos, infraestructura y equipamiento de sus cadenas, misionales y críticas, de suministro y producción.

Dichas cadenas de valor que, por su imposibilidad de ser sustituidas o remplazadas o, por lo menos, no suplidas de manera fácil, rápida y ágil, y, en todo caso, con la inmediatez y oportunidad que requiere una situación compleja y difícil, constituyen y son la razón, para que dichas cadenas de producción que forman parte de industrias esenciales, como el sector flexográfico, sean fundamentales para la sociedad, la economía y el país, debido al significativo impacto que ocasiona su paralización, temporal o definitiva, sobre otras infraestructuras de producción críticas de otras industrias igualmente necesarias y esenciales, como se infiere de lo afirmado por [10] respecto a la llegada de los avances tecnológicos, la modernización y la digitalización, a este sector industrial.

De otra parte, estas mismas circunstancias y fenomenología afectan, particular y especialmente, a las PYMEs de la industria flexográfica que, son sujetos de mayor riesgo informático y de gran y permanente interés de parte de los ciberatacantes, en razón a su condición de empresas muy vulnerables económica y financieramente y, por tanto, con limitados y escasos recursos disponibles, para atender todo tema relacionado con la seguridad de la información, la seguridad informática y la ciberseguridad. Consecuentemente, esto hace a las PYMEs muy sensibles a daños, suspensión de actividades, paralizaciones y otras eventualidades relacionadas con sus

procesos productivos que, incluso, las puede llevar a procesos legales de declaración de quiebra, como afirma [2].

En efecto, debido a su restringida capacidad presupuestal y de inversión, tanto para procesos esenciales de naturaleza administrativa, operativa y de producción, como, también, para adquisición de soluciones tecnológicas, a lo cual se añan las grandes limitaciones y disponibilidad de talento humano especializado en ciberseguridad, todos ellos motivos por los cuales, en este punto, y con enfoque en la protección y resiliencia de las cadenas productivas de la industria flexográfica, es importante considerar los siguientes términos informáticos cuya definición conceptual se soslaya en [2], [11], [15], [16] y [28], y que son, básicamente, la ciberseguridad y el riesgo cibernético.

2.1.2 Industria, infraestructura TI y seguridad informática

Sobre la sinergia de industria y ciberseguridad, afirman [15], [16] y [28] que, en el contexto moderno actual, donde, la industria toda, incluido el sector flexográfico, viene experimentando una acelerada transformación digital y, en la cual, la automatización de los procesos productivos es ya una característica intrínseca, la seguridad informática se ha convertido en un pilar, tan fundamental como obligado, para garantizar la productividad, la continuidad, la resiliencia y la sostenibilidad de las cadenas de producción y esta afirmación, trasciende la industria flexográfica y se extiende a todos los sectores industriales de la economía real, a lo cual, ningún segmento está exento, hoy por hoy, pues los ciberataques no tienen respeto alguno por ningún tipo de empresa, organización, sector, entidad, institución, ni del ámbito público, ni tampoco del sector privado.

En este sentido, como se infiere de [15], [16], [17], [18], [26] y [27], la interconexión creciente de los sistemas informáticos asociados a la gestión de la cadena productiva, sin olvidar, y aunque no están incluidos en el alcance de esta tesis de maestría en seguridad informática, a los sistemas operativos industriales (ICS), las redes de tecnología operacional (OT) y las plataformas de gestión empresarial, todos los cuales, tienen conectividad casi permanente con el ciberespacio y con redes externas,

aumentando sustancial y significativamente la superficie de riesgo y exponiendo a las organizaciones ante acciones cibernéticas maliciosas que, eventualmente, pueden comprometer la confidencialidad de los datos, la integridad de las líneas de producción y la disponibilidad de los servicios críticos como se desprende de [38].

Igualmente, una falla tecnológica, una contingencia técnica, una calamidad o un desastre, como bien afirman [16] y [18], también, pueden impactar sobre la normal operación de las cadenas productivas en las industrias, asunto particularmente importante y de obligada atención, sobremanera en el caso del sector flexográfico, considerado como una industria esencial, desde la pasada época de pandemia de Covid-19 donde se demostró la criticidad de sus procesos y de su cadena productiva.

Vale resaltar en este punto que, en la actualidad, aún el sector flexográfico, al igual que el sector convertidor y de transformación de plástico, no son formalmente reconocidos, de manera oficial, como infraestructuras críticas a nivel mundial, regional, ni local, pero, su esencialidad ya fue demostrada en momentos de crisis, como la del Covid-19, y garantizan que, en un futuro próximo, este paso será dado por parte de los gobiernos y los organismos y entes internacionales.

Consecuentemente, y según se desprende de las contribuciones [12] y [26], de la implementación de un modelo de ciberseguridad que incluya políticas robustas de seguridad informática permite proteger infraestructuras industriales frente a amenazas como la ingeniería social, el malware, el ransomware, los accesos no autorizados y sabotajes digitales, garantizando así la continuidad y la resiliencia operativas, el cumplimiento normativo y la confianza de clientes, proveedores, accionistas, socios comerciales y terceros interesados.

En este sentido, la seguridad informática ya no es más un mero componente auxiliar u opcional para las organizaciones, sino, en cambio, un elemento estratégico e imprescindible que debe integrarse, desde el diseño hasta la operación, de cualquier entorno industrial y, en particular, debe ser considerado como aspecto de protección fundamental de la cadena de producción de una industria como la flexográfica, considerada, en la actualidad, como crítica para la sociedad, la economía y el país.

2.1.2.1 Ciberseguridad

Respecto a la conceptualización de ciberseguridad, como afirman [15] y [16] y [18], se puede aseverar que se trata del conjunto de prácticas, técnicas y tecnologías dedicadas a proteger los activos, infraestructuras, sistemas, redes, información y datos, frente a la ocurrencia de amenazas cibernéticas tales como ataques maliciosos, accesos no autorizados y daños informáticos intencionados o accidentales.

En efecto, tal como aseveran [12], [13], [19], [25] y [27], el objetivo principal de la ciberseguridad es asegurar que la información digital se mantenga confidencial, es decir, que solo esté disponible para aquellos que tienen el permiso adecuado; que se conserve íntegra, lo que significa que no se altere o manipule sin autorización; y que siempre se encuentre disponible, lo que garantiza que los datos y servicios puedan ser accedidos y utilizados cuando sean necesarios por usuarios debidamente autorizados.

Este enfoque integral de ciberseguridad se aplica, como profesan [12] y [38], tanto en el ámbito personal, como marco de lo empresarial y es fundamental para la protección de la infraestructura crítica y la continuidad y la resiliencia operativa de cualquier organización industrial en el entorno digital actual, de la cual la cadena productiva de la industria flexográfica no es la excepción, sino uno de tantos sectores que adolecen la necesidad urgente de mejorar la ciberseguridad.

2.1.2.2 Riesgo informático

De otra parte, el riesgo informático, según [16] y [27], se trata de la capacidad de un sistema computacional de sufrir daños, impactos o pérdidas y se debe a la exposición de este, ante diversas ciberamenazas que pueden materializarse afectando e impactando la funcionalidad y operatividad de dicho sistema informático. La gestión del riesgo es particularmente importante, sobremanera, cuando se trata de sistemas computacionales asociados a la cadena productiva de una empresa. Este tipo de riesgos pueden manifestarse, como bien observan [12]

y [25], en forma de ataques cibernéticos, fallos técnicos o errores humanos que comprometen la seguridad de la información y que, eventualmente, pueden afectar el normal funcionamiento de la cadena de valor, por su impacto en la continuidad operativa y la resiliencia organizacional de una empresa.

De otra parte, como afirma [18], la correcta gestión del riesgo es fundamental para minimizar el daño potencial que puede sufrir una compañía y, en especial, necesaria para garantizar la continuidad operativa y la resiliencia organizacional de los sistemas informáticos asociados a la cadena de producción esencial de las empresas, pues, al final del día, estos sistemas computacionales, en su gestión de mando y control de las líneas de producción esenciales, operan en un entorno digital, como el actual, complejo, dinámico y cambiante, donde proliferan las ciberamenazas para las infraestructuras críticas, sin ser excepción, las cadenas de producción de las PYMEs y compañías de la industria flexográfica, independientemente de su tamaño y subsector productivo.

Al respecto, y según coinciden [13], [15], [16], [18], [19], [25] y [27], el riesgo informático nunca puede ser eliminado por completo, por lo cual existen diversas estrategias para gestionarlo de manera efectiva. En efecto, el tratamiento del riesgo informático se puede gestionar con estrategias como la mitigación, que busca reducir la probabilidad o el impacto del riesgo; la transferencia, desplazándolo a un tercero; como es el caso de una póliza de seguros u otras formas de externalizar las consecuencias de una eventualidad; de otra parte, está la aceptación, donde se decide intentar convivir con el riesgo; y, finalmente, pero, no menos importante, está la opción de la evitación, que implica tomar medidas para eliminar la exposición a ciertas amenazas; y dado que, su aplicabilidad depende de las características y particularidades de cada compañía.

Este mayor nivel de exposición y de vulnerabilidad informática que, potencialmente, pueden afectar a sus irremplazables infraestructuras críticas de producción, según [16], hacen imprescindible que las PYMEs de la industria flexográfica implementen arquitecturas de ciberseguridad efectivas y adaptadas a su realidad, condiciones, circunstancias y necesidades particulares, con especial enfoque en la protección

de los sistemas informáticos que gestionan, operan y controlan sus cadenas de producción, considerándolos como elemento clave para su supervivencia.

Todo lo anterior, por cuanto, la industria flexográfica presenta la condición de tener una cadena productiva crítica en continuo proceso de digitalización, como se infiere de [17], lo cual genera mayor nivel de riesgo informático y una mayor exposición ante amenazas cibernéticas o, también, vale anotar, mayor probabilidad de explotación de vulnerabilidades o posible ocurrencia de fallas tecnológicas o contingencias de naturaleza técnica, a lo cual se aúna la complejidad y dificultad de remplazar, en el corto plazo, su cadena crítica de producción.

2.1.2.3 Controles

Los controles informáticos, según [15], [16], [18], [25], [26] y [27], son medidas diseñadas para proteger los activos de información frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad. Estos controles, según [25], pueden ser de tipo preventivo, detectivo, correctivo o disuasivo y se implementan con el objetivo de reducir la probabilidad y el eventual impacto de los incidentes de seguridad.

Los controles cumplen un rol fundamental en la constitución de un modelo de ciberseguridad, puesto que permiten mitigar los riesgos identificados en la matriz de riesgo y en el mapa de calor, alineando la gestión de ciberdefensa y la operación de la infraestructura informática asociada a la cadena productiva crítica con los requisitos normativos derivados de los estándares internacionales ya mencionados. Los controles permiten establecer las barreras de protección contra eventos indeseados como accesos no autorizados, pérdida de datos, fuga de información, interrupciones operativas y, también, vale mencionar, contra errores humanos, ya estos sean de naturaleza involuntaria o, por el contrario, intencionales.

Su según afirman [15], [16], [18], [19], [25], [26] y [27], su importancia radica en que no solo fortalecen la postura de seguridad de una organización, sino que, también, facilitan el cumplimiento legal y contractual, generan confianza entre clientes,

proveedores, accionistas, auditores y terceros, pero, sobre todo, dan forma definida, específica y determinada, a la defensa cibernética como tal. En esencia, los controles informáticos son el mecanismo operativo que convierte la política de seguridad cibernética en acciones concretas y medibles, reduciendo el riesgo de manera eficaz, efectiva y sostenible.

A efectos metodológicos y técnicos de esta tesis de maestría en seguridad informática y, según los lineamientos de [25], la detallada revisión y consideración de los diversos estándares internacionales y de las buenas prácticas de seguridad informática, acorde con los resultados del análisis y evaluación del riesgo cibernético encontrado, se ven reflejados y permitieron la selección de los controles pertinentes, que están consignados más adelante, en el capítulo 4 de resultados de esta tesis de maestría y que, conforman el resultado protectivo y defensivo práctico e implementable del modelo de ciberseguridad desarrollado para la infraestructura IT asociada a la cadena de producción crítica de las PYMEs y empresas del sector flexográfico (o de otras industrias similares).

2.1.2.4 Ataque informático o ciberataque

Respecto a los ataques informáticos, conocidos comúnmente como ciberataques, según afirma [15], se trata de acciones de índole ofensiva, claramente mal intencionada y de naturaleza deliberada, planeadas, diseñadas y ejecutadas por individuos o grupos con competencias técnicas de diversos grados, mediante el uso de sistemas computacionales e informáticos, redes o dispositivos electrónicos o digitales.

El objetivo principal y claro de los ciberataques, según afirma [16], es comprometer la confidencialidad, integridad o disponibilidad de la información digital (triada de la CIA), ya sea para robar datos sensibles, extorsionar, robar, obtener ganancias económicas de sus víctimas, espiar actividades o, simple y llanamente, ralentizar, dificultar, interrumpir o colapsar el funcionamiento normal de servicios informáticos esenciales y, como ejemplo del caso en estudio, impactar la infraestructura cibernética de gestión de las cadenas de producción críticas de la industria flexográfica.

Resumiendo, y según se infiere de [27], un ciberataque es una acción ladina deliberada que aprovecha una vulnerabilidad o debilidad en un sistema computacional para que un actor de amenaza, o ciberdelincuente, se infiltre a través de un vector de ataque específico con el propósito clave de ejecutar una carga útil maliciosa que comprometa la triada de la CIA de un sistema informático, generando un impacto negativo que puede ir desde el robo de información sensible hasta la interrupción total de servicios digitales esenciales.

2.1.2.5 Infraestructura de producción crítica

Por otra parte, como ya se comentó y como, también, se infiere de las investigaciones de [1], [17], [33], [40] y [41], el sector flexográfico es parte fundamental del sector real de la economía, razón por la que sus procesos, infraestructura y equipamiento productivo son considerados, desde la pasada pandemia de Covid-19, como prioritarios y esenciales, aun cuando, actualmente no están formalmente incluidos dentro de la definición oficial de infraestructura crítica, como al respecto indica [16]. La Fig. 4 ilustra el web site típico de una PYME o empresa del sector flexográfico.

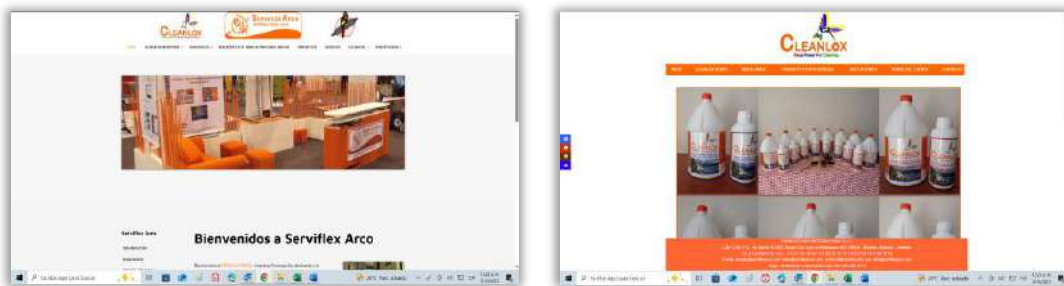


Fig. 4 Web sites corporativos de una empresa del sector flexográfico.

Nota. Web sites empresa del sector flexográfico. Fuente: tomado de [44].

Dicho sector, como se infiere de [10] e indirectamente de [41], [42] y [43], incluye las industrias de la flexografía o de impresión flexográfica, siendo un sector especializado en la producción de productos primordiales, insustituibles e irremplazables en las cadenas logísticas que, igualmente y de manera similar a la industria flexográfica, cuentan con infraestructuras productivas tan críticas como esenciales y cuyos productos

son esenciales e indispensables para otras cadenas logísticas y de suministros de otras industriales críticas, como por ejemplo, la alimentaria, la farmacéutica, la de bienes, productos y mercancías básicos y de primera necesidad, entre muchas otras más.

Reconfirmando lo anterior y resaltando la importancia y el avance de la flexografía, apunta [17] y, también, se infiere del trabajo de [43] que, esta industria esencial, se ha convertido en el proceso de impresión de empaques, bolsas, cajas, etiquetas y envases, con mayor crecimiento y desarrollo tecnológico en su segmento sectorial, pues, en efecto, este sector productivo ha venido siendo principalmente impulsado, en su desarrollo y renovación, principalmente, por la modernización derivada de las innovaciones tecnológicas en sus líneas de producción, con especial importancia de las nuevas tecnologías, como el IoT y la AI y, también, por la incorporación de la propia digitalización en las actividades corporativas y organizacionales cotidianas y como parte fundamental de los procesos productivos empresariales.

Estas tecnologías, conforman todas ellas, el gran avance que, se han venido incorporando paulatina, pero, firmemente, a la industria flexográfica desde tiempo atrás, pero, particularmente, durante, la última década; tendencia que, como indican [15], [18] y [26], de seguro, continuará de manera sostenida e imparable en el futuro venidero. Es menester resaltar en este punto que, igual circunstancia acontece con otras industrias y sectores productivos similares, por lo cual, el modelo desarrollado en esta tesis de maestría, guardadas las proporciones y ajustes debidos, también, es aplicable a otras industrias similares.

Sobre la difusión de la tecnología en la cadena de producción flexográfica, continúan afirmando [1], [10], [17] y [42] que, ha crecido significativamente y que su incorporación en los procesos industriales es una realidad actual, originada en la capacidad sectorial de adaptarse a la modernización y a las nuevas tendencias de automatización y digitalización derivadas de un alto nivel de competencia y de las demandas del mercado actual, pues, toda ellas priorizan el incremento en la productividad, la reducción de costos de producción, tiempos de entrega más cortos y la mejora en la calidad del producto final.

Este crecimiento en sofisticación y avance tecnológico ha sido posible gracias a un proceso evolutivo que incluye, no solo los avances en la modernización de equipamientos, sino, también, en la creciente automatización de los procesos productivos y hasta en los avances en los materiales y sustratos utilizados en los procesos de producción. La flexografía, por lo tanto, no se ha quedado al margen de los desarrollos tecnológicos más recientes.

En efecto, la industria flexográfica ha venido integrando, de manera progresiva, la digitalización y las nuevas tecnologías en todos los aspectos esenciales de su cadena de producción, como bien apunta [17]. Según [6], esta modernización, desde la aplicación de los sistemas de control digital (SCD) en las industrias energéticas, de finales del milenio anterior, ha permitido que, muchas industrias, incluido el sector flexográfico, no solo mantenga su competitividad, sino que, también, mejore significativamente su capacidad para cumplir con las exigencias del mercado global en términos de eficiencia y sostenibilidad, consolidándose como la opción de producción preferida en su segmento industrial (en comparación con otros sectores productivos como el rotograbado).

Debido a lo anterior y, particularmente, sobre los efectos del desarrollo, la modernización y la digitalización en los procesos críticos y esenciales del sector flexográfico, plantean [17] y [43] que la cadena de producción es, y continuará siendo, un factor central y básico en el ámbito de la industria por su naturaleza esencial, en razón a que, por definición, se trata del conjunto de etapas a través de las cuales, un producto o servicio, se desarrolla desde su concepción, incluyendo las fases de creación y diseño iniciales, su progreso, hasta su llegada al consumidor o usuario final.

Por tanto, cuando se trata de sectores reales de la economía y, en particular, de aquellos considerados críticos o, por lo menos, esenciales, como lo es la cadena de producción de la industria flexografía, todo lo relacionado con su seguridad informática desempeña un factor clave y trascendental para la estrategia organizacional y para la operación empresarial, como reafirman [1] y [10] y se infiere de investigaciones en otros sectores, como plantea [45]. Complementando lo anterior, bien afirman [12] y [16], que las organizaciones requieren de adaptabilidad, flexibilidad y de dotar de continuidad

operativa y de resiliencia a sus procesos e infraestructuras críticas, pues se necesita garantizar la funcionalidad productiva a fin de asegurar la sostenibilidad, supervivencia, crecimiento y prosperidad empresarial en el largo plazo.

De otro lado, como se infiere en [11], [12] y [13] y por extensión, para el caso de la cadena de producción del sector esencial de la flexografía, en su calidad de industria protagonista, imprescindible e irremplazable (por lo menos en el corto plazo), en el proceso manufacturero de los empaques, embalajes, envases, cajas, etiquetas y muchos otros productos básicos y de primera necesidad para las cadenas logísticas y de suministro de otras industrias críticas, pues, toda organización, en especial todas aquellas categorizadas como PYMEs, requieren del desarrollo y fortalecimiento de su capacidad para prever, detectar, responder, mitigar, recuperar, resistir y superar incidentes cibernéticos.

De otra parte, como afirman [15], [16] y [26], estos procesos de ciberseguridad facilitan de manera simultánea, el fortalecimiento y mejoramiento de la infraestructura y de los sistemas informáticos propios, con el objetivo de gestionar adecuadamente, cualquier potencial eventualidad maliciosa o suceso fortuito, ya sean estos derivados de ciberataques o ya causados por acontecimientos inesperados como fallas tecnológicas, contingencias técnicas, calamidades o desastres informáticos.

En efecto, las PYMEs de la industria flexográfica, requieren dotar, mejorar o fortalecer, la resiliencia informática de sus procesos productivos y organizacionales como plantean [19] y [27], en el sentido que, la clave y el eje central del éxito, en toda la actividad empresarial de largo plazo, se apoya y se sustenta en la resiliencia, como indirectamente se pudo observar de la Fig. 5, donde se muestra cómo la estrategia de ciberseguridad debe ser profiláctica, proactiva, y al igual que se cuida la salud humana, debe ser guiada por etapas estratégicas muy dirigidas a una actitud que evite la reactividad o tener que aceptar las consecuencias de no estar preparados para gestionar adecuadamente la ciberdefensa de los sistemas informáticos.

En efecto, y tal como recomienda [37], en la actualidad, la realidad de las empresas ya no se trata de si van a ser atacadas o no, sino, más bien, de cuando van a ser atacadas, razón por la cual, la ciberseguridad debe ser asumida como una medida sanitaria

necesaria para las organizaciones, más cuando se trata de industrias esenciales, como el sector industrial de la flexografía, altamente vulnerable ante .



Fig. 5 Prevención en seguridad informática, analogía con sector salud.

Nota: Analogía con la infraestructura esencial del sector salud. Fuente: tomado de [46].

Esta es la razón por la cual, como bien corroboran [12], es necesario asegurar siempre, la acertada gestión de la continuidad de los procesos misionales de carácter productivo y robustecer la resiliencia operativa de los sistemas informáticos de la cadena de producción, como también, de los propios procesos internos de otras naturalezas al interior de las empresas y PYMEs de este importante sector industrial del cual hace parte la flexografía.

En este sentido, sobre los efectos de las TIC en las cadenas productivas, afirma [45], que mejoran la eficiencia de las cadenas de producción. Sin embargo, coinciden en que, su utilización como factor o elemento cada vez más importante, frecuente y permanente, aumentan la superficie de exposición e incrementan el nivel de riesgo ante ciberataques y amenazas informáticas, razón por la cual, se destaca la necesidad y la importancia estratégica para toda organización, de asegurar debidamente la resiliencia de los procesos misionales de su cadena de valor.

Al respecto, están en completo acuerdo [16], [18], [19] y [27], al resaltar la importancia de la integración de la seguridad informática como eje fundamental en la cadena productiva de las compañías y organizaciones de la economía real, sin importar el tipo de industria de que se trate, o del tamaño empresarial y, en particular, cuando se trata del caso de una PYMEs, pues toda empresa, más temprano que tarde, será objeto de alguna tentativa de ciberataque. Es importante resaltar que, las infraestructuras críticas son componentes esenciales en el funcionamiento de una sociedad moderna, abarcando una amplia gama de sistemas, estructuras y activos cuya interrupción, paralización, suspensión o destrucción (parcial o completa), tendría un impacto significativamente negativo no solo en la seguridad, sino, también, en la economía, la salud pública y el bienestar general de la sociedad, la nación o el estado, según se desprende de las apreciaciones de [15], [16], [18], [19] y [27].

De esta forma, se puede considerar que la criticidad de las infraestructuras críticas se fundamenta en que se definen como los sistemas físicos o virtuales vitales, esenciales, insustituibles e indispensables para el funcionamiento de una sociedad, una nación o un estado que incluyen, pero, no se limitan, a redes de energía eléctrica, agua, gas y saneamiento, redes de telecomunicaciones, sistemas de transporte, infraestructuras de servicios de salud, sistemas de servicios financieros y, más recientemente, las cadenas productivas de las industrias esenciales, como la alimentaria, la farmacéutica, la de bienes básicos de consumo, la de artículos y productos de primera necesidad, entre otras y sus sectores asociados como, en particular, la flexografía (ver Fig. 9), aun cuando, actualmente, aun no esté formalizada y legalmente reconocida, por parte del estado colombiano, como infraestructura crítica, como bien apuntan [15] y [18].

A continuación, la Fig. 6 muestra la cadena de producción de una empresa perteneciente a la industria flexográfica y dedicada a la producción de empaques y embalajes registrada por [47]. En ella se puede apreciar una cadena de producción típica, caracterizada por máquinas modernas, controladas por medio de una infraestructura informática y computacional con conexión permanente al ciberespacio, incluidas redes externas propias, de las casas fabricantes de sus líneas de maquinaria, de servicios tecnológicos externos, de terceros interesados como grandes clientes,

entre otros muchos, las cuales, acorde con [6], [10], [17], [23], [24] y [49] presentan gran vulnerabilidad y están expuestas a riesgos cibernéticos.



Fig. 6 Infraestructura de producción de una empresa esencial del sector flexográfico

Nota. Planta típica de producción flexográfica crítica. Fuente: tomado de [47].

Al respecto [38], enfoca con mayor precisión y concisión, el concepto de infraestructura crítica, como aquella cuyo funcionamiento es indispensable y cuya interrupción, paralización, ya temporal o definitiva o, incluso la destrucción total de la misma tendría un grave y significativo impacto en los servicios esenciales de la sociedad y la economía, sin posibilidad de soluciones alternativas u opciones de remplazo de corto plazo. Al respecto, y como puede observarse de lo afirmado por [15], [16], [18], [19] y [51], las infraestructuras críticas se refieren a procesos irremplazables de naturaleza esencial para las empresas, las industrias, la economía, la sociedad, los estados y, por supuesto, y aún más importante, para las personas, en razón a los impactos que pueden tener en la vida cotidiana de los seres humanos.

Según [16] y [48], esta definición de infraestructura crítica se extiende a las cadenas productivas esenciales, pues, requieren del aseguramiento de su resiliencia operativa, para hacer más fácil su restablecimiento y recuperación, a condiciones de normalidad, cuando sufren eventualidades y, simultáneamente, para permitir dotarlas de resistencia, flexibilidad y adaptabilidad para enfrentar condiciones de cambio o de incertidumbre, facilitando la mitigación y reducción del nivel de riesgo informático de manera integral, tanto para la empresa como para su cadena de producción.

2.1.2.6 Continuidad operacional y resiliencia de la infraestructura TI asociada a la gestión de la cadena de producción crítica de la industria flexográfica

En la industria flexográfica, garantizar la continuidad operacional y la resiliencia de la infraestructura informática asociada a la gestión de la cadena productiva es un aspecto tan esencial como crítico para la estabilidad, desempeño y eficiencia de la producción y, también, para la sobrevivencia de una empresa, en particular, si se trata de una PYME, cuya capacidad de respuesta, ajuste y superación de eventos cibernéticos es mucho más limitada, según afirman [23], [24] y [49].

Igualmente, como consigna [17] y [49], la industria flexográfica depende en gran medida de sistemas IT que, gestionan, operan y controlan, no solo los procesos de impresión, sino, también, otras etapas de la producción como son el diseño, la pre prensa, el acabado, el aprovisionamiento de insumos, la programación de producción, el control de calidad, entre otros. Ante este panorama, cualquier interrupción en los sistemas informáticos puede generar trastornos en la producción que se pueden reflejar como pérdidas económicas significativas, incumplimientos contractuales, pérdida de clientes y daños reputacionales, que pueden trascender el ámbito de las empresas del sector y conocerse en otros mercados y escenarios de la economía (Bancario, asegurador, fabricantes internacionales, clientes, et al).

La continuidad operacional en la flexografía implica la implementación de una estrategia de seguridad informática que permita mantener las operaciones incluso ante incidentes imprevistos, como fallas tecnológicas, ataques cibernéticos o

desastres naturales y, por tanto, la adopción de un enfoque basado en la gestión de riesgos, pero, sobremanera, la adopción de las premisas y recomendaciones de estándares internacionales, como ISO 22301 [52], ISO 22361 [53], ISO 22316 [54] y, también, el propio marco NIST 2.0 CSF [4], resultan de esencial importancia, permitiendo a las organizaciones, la rápida y oportuna identificación de vulnerabilidades, así como el establecimiento de mecanismos prácticos y adaptables de respuesta a incidentes que sean efectivos y eficaces.

En este sentido, según [16] y [27], medidas como la redundancia de sistemas, el almacenamiento seguro de datos y la automatización de respaldos son factores de gran contribución a efectos de mitigar el impacto de posibles interrupciones. Por otro lado, la resiliencia informática en la industria flexográfica es otro factor primordial, pues se refiere a la capacidad de los sistemas informáticos para adaptarse y recuperarse rápidamente de incidentes cibernéticos, minimizando el tiempo de inactividad y garantizando la continuidad del flujo de trabajo, la cual, es una capacidad que, por supuesto, se refleja en la cadena de producción de la organización.

En este aspecto, la implementación de soluciones de detección y respuesta ante amenazas (EDR), como plantea y [27], el monitoreo constante de la red como sugiere [26], y la capacitación continua del personal en ciberseguridad como propone [19], fortalecen la capacidad de adaptación y flexibilidad de las empresas, incluidas las PYMEs, para enfrentar ciberataques y fallos tecnológicos, haciéndolas, en general, más resilientes.

Así pues, tal como apunta [12] y reconfirma [18], en un entorno industrial donde los márgenes de error son reducidos y la demanda de producción es tan constante como esencial, la combinación de robustez operacional y resiliencia informática no solo propende por la protección de los activos digitales de la empresa (ver lineamientos en [50], [51] y [52]), sino que, también, motiva la adopción e implementación de estándares internacionales de amplia aceptación, en aras de asegurar la continuidad y la resiliencia de la cadena productiva garantizando la satisfacción del cliente.

Al respecto apuntan de [15], [16], [27] y [49], que la inversión inteligente y razonada en infraestructura tecnológica segura, junto con la adopción de mejores prácticas en ciberseguridad y prácticas de recuperación ante desastres, se convierte en un factor diferenciador para la competitividad y sostenibilidad de las empresas, en un mercado globalizado y muy competido, como el mercado actual, particularmente en industrias esenciales, como el sector flexográfico.

2.1.2.7 Infraestructura TI

Como bien afirman [15], [16], [18] y [27], la infraestructura de tecnologías de la Información (TI) se define como el conjunto de combinado de recursos lógicos y físicos, compuesto por hardware, software, recursos de red y diversos servicios, que permiten el procesamiento, almacenamiento y flujo de datos e información. El sistema TI representa la base tecnológica sobre la cual una organización despliega sus aplicaciones y procesos de negocio, permitiendo la recolección, el almacenamiento, el procesamiento y la distribución de datos de manera centralizada y eficiente.

Esta arquitectura incluye desde los servidores locales y servicios en la nube hasta las estaciones de trabajo, Para el caso de la industria flexográfica, la infraestructura TI permite el procesamiento de ordenes de trabajo, programa de producción, archivos de diseño gráfico, gestión de las bases de datos de los clientes y sus órdenes, entre muchos otros. En un modelo de ciberseguridad, la infraestructura TI actúa como el perímetro de soporte que garantiza que las órdenes de producción y los archivos digitales lleguen de forma íntegra a la planta, protegiendo la propiedad intelectual del diseño y la continuidad del negocio.

Por lo anterior, entre los principales aspectos de seguridad informática a considerar en la ciberdefensa de la infraestructura TI de la industria flexográfica se tienen la disponibilidad, la integridad y la confidencialidad de los datos. Se destacan factores clave como la seguridad de las redes corporativas (LAN/WLAN), la gestión de identidades y accesos para proteger los activos de información críticos, y la protección de los terminales (endpoints) frente a amenazas como el malware y el

ransomware, que podría paralizar la cadena crítica de producción. Por las razones anteriormente expuestas relacionadas con el alcance de esta tesis, al excluir los sistemas OT, el enfoque investigativo se desplazó, con base en los estándares internacionales y buenas prácticas de seguridad, hacia el endurecimiento de los sistemas operativos, el cifrado de archivos en tránsito y la implementación de protocolos de respaldo robustos que, entre otros controles que se proponen, permitan la recuperación ante desastres y ciberataques.

2.2 Estado del arte

En el siguiente aparte se condensa el estado del arte en el tema bajo el soporte de trabajos e investigaciones de maestría y doctorado que cubren temáticas similares a la tratada en esta tesis de Maestría. Al respecto, en su investigación "*Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad*", [13] plasma las pautas para construir un modelo de ciberseguridad cuyo principal fundamento es la evaluación y el análisis del riesgo informático con claro enfoque en lograr una pertinente gestión y manejo de eventualidades e incidentes informáticos, a través de realizar la selección de los estándares, normas, marcos y demás herramientas apropiadas que, faciliten robustecer el proceso atención y tratamiento de incidentes informáticos, para lo cual, el autor se apoya en criterios selectivos de priorización y categorización que permitan definir la criticidad de los activos computacionales.

En este punto vale la pena resaltar que se trata del caso de compañías que ofrecen servicios informáticos. Así, el modelo de ciberseguridad propuesto se cimenta en la norma ISO 27005 [21] que establece los procedimientos necesarios para el manejo y detección de riesgos de seguridad, abordando en primera instancia un proceso de identificación de activos para, en una segunda etapa, analizar los diversos escenarios de riesgo. Posteriormente, [13] procede a definir los controles idóneos en aras de lograr una adecuada mitigación de impactos producidos por la materialización de los riesgos. Finalmente, el autor desarrolla su propuesta de modelo de ciberseguridad empresarial, la

cual per se ya incluye todos los aspectos antes mencionados, como la evaluación y análisis del riesgo con priorización de puntos críticos o el manejo y la respuesta a incidentes, ambos bajo el imperio del mejoramiento continuo, ciclo PHVA y la selección de controles adecuados para la protección del sistema informático.

En otra interesante investigación aplicada, intitulada “*Modelo de ciberseguridad en las unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico nacional*”; en la que [53] propone un modelo de ciberseguridad para el proyecto Sistema Inteligente de Supervisión y Control Avanzado del Sistema Interconectado Nacional colombiano, centrado en la protección de la infraestructura de medición fasorial frente a ciberataques.

El modelo incluye la evaluación y análisis de riesgo informático mediante una metodología tradicional y establece controles específicos, para reducir dicho nivel de riesgo, sobre las unidades de medición fasorial. Además, se implementa un ambiente de prueba para validar el impacto de los controles de seguridad en la mitigación de ciberamenazas, como ataques DDoS, malware, APTs, secuestro de información y ataques de suplantación. El objetivo final es fortalecer la resiliencia informática del sistema ante amenazas, asegurando la continuidad y resiliencia operativa del sistema eléctrico colombiano frente a un amplio espectro de ataques cibernéticos.

En otro trabajo investigativo sobre “*La protección de las infraestructuras críticas*”, [54] presenta una revisión de las amenazas cibernéticas y el potencial riesgo de la infraestructura crítica, la cual puede verse vulnerada en caso de ciberguerra. Se hace especial énfasis en el sistema eléctrico nacional y se presentan los nuevos desafíos tecnológicos relacionados con este tipo de infraestructuras críticas automatizadas e interconectadas al ciberespacio.

La investigación de [54], también, destaca a la ciberdefensa como estrategia necesaria para la protección de las infraestructuras críticas de los estados y presenta el nuevo contexto político y estratégico producido por la aparición de la ciberguerra y como la importancia de dichas infraestructuras críticas, se torna en un factor relevante en razón a las nuevas amenazas cibernéticas. Importante resaltar que, sobre el caso de protección de infraestructuras críticas, también, se proponen otras visiones como la de [55], que

aportan otros interesantes elementos para un modelo de ciberseguridad como él propuesto.

En la investigación titulada "*Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa*", [12] desarrollan la construcción de un modelo de ciberseguridad basado en el análisis de riesgos, enfocado en el fortalecimiento de la gestión y manejo de incidentes de informáticos para todas las operaciones que ofrecen servicios informáticos.

En aras de cumplir esta meta, [12] plantean la detección de los riesgos para empresas que ofrecen este tipo de servicios informáticos, y al efecto se soportan en la norma ISO 27005 [21] que establece los procedimientos necesarios para el manejo y detección de riesgos de seguridad, comenzando por un fase de levantamiento, identificación y valoración de activos seguido, a continuación, por una etapa de análisis de escenarios de riesgos, mediante lo cual posibilitan la definición de los controles adecuados que mitigaran los eventuales impactos de la materialización de un riesgo específico sobre la infraestructura informática de la compañía.

Es importante anotar que el enfoque clave de este aporte investigativo de [12] estriba en garantizar el adecuado manejo de incidentes de ciberseguridad, lo cual se consolida por la correcta selección de las normas y estándares de ciberseguridad adecuados los cuales deben ser seleccionados bajo criterios selectivos de prioridad e importancia, en riesgos críticos y en controles adecuados, a fin de generar los cimientos de construcción del modelo de ciberseguridad planteado para la infraestructura informática corporativa de tal manera que asegure la protección y aseguramiento de la confidencialidad, integridad y seguridad de la información como objetivo fundamental.

De otro lado, en el trabajo de investigación "*Mejora de procesos de la ciberseguridad aeronáutica mediante un marco de trabajo de madurez*", [14] presentan una revisión exhaustiva y muy detallada de las metodologías para evaluar la madurez en ciberseguridad de la infraestructura crítica de la red aeronáutica nacional. Basado en estos resultados, producto de su indagación y esfuerzo investigativo, el autor propone un marco de trabajo que integra objetivos de ciberseguridad aeronáutica con estándares internacionales, como

norma ISO 27001 [3], NIST 2.0 CSF [4] y la metodología COBIT (descrita por [56]), con el fin de mejorar la madurez en la seguridad informática del sector.

En este trabajo de investigación, [11] identifican trece (13) objetivos asociados a ciento veinte (120) capacidades operativas, distribuidas en seis (6) niveles de madurez, que generan seiscientos (600) diversos requerimientos. El estudio, validado por expertos y directivos de la industria aeronáutica, subraya la importancia de la evaluación de riesgos, la gestión de incidentes y la adaptación a cadenas productivas específicas. Además, resalta la relevancia de la continuidad operativa y la resiliencia organizacional como pilares fundamentales para proteger infraestructuras críticas. En este modelo, [14] proponen una visión estratégica que utiliza estándares internacionales para enfrentar los desafíos de ciberseguridad en un sector vital para el transporte global.

Finalmente, en otro trabajo investigativo sobre “*Revisión de ciberdefensa de infraestructura crítica*”, [40] presentan una revisión de las amenazas cibernéticas actuales y el potencial riesgo de la infraestructura crítica, la cual puede verse vulnerada en caso de ciberguerra. Se hace especial énfasis en el sistema eléctrico nacional y se presentan los nuevos desafíos tecnológicos relacionados con este tipo de infraestructuras críticas automatizadas e interconectadas al ciberespacio. La investigación, también, destaca a la ciberdefensa como estrategia necesaria para la protección de las infraestructuras críticas de los estados y presenta el nuevo contexto político y estratégico producido por la aparición de la ciberguerra y como la importancia de dichas infraestructuras críticas, se torna en un factor relevante en razón a las nuevas amenazas cibernéticas. Importante resaltar que, sobre el caso de protección de infraestructuras críticas, también, se proponen otras visiones como las de [57] y [58], que aportan otros interesantes elementos para un modelo de ciberseguridad como el propuesto.

Así pues, se desprende como conclusión de la revisión del estado del arte que, la protección de los sistemas de TI no es solo una medida técnica, sino una columna vertebral estratégica para la estabilidad de la sociedad y la nacional puesto que su contribución al fortalecimiento de la continuidad operativa en sectores productivos de alta complejidad es esencial. Integrar marcos un prototipo cibernético protectivo para la infraestructura TI asociada a los procesos y cadenas de producción de una industria como la flexográfica, es tan necesario como se muestra de las contribuciones aplicadas en otros sectores.

En este punto, es importante resaltar que, aunque la convergencia entre sistemas TI e infraestructuras OT es una tendencia creciente en la industria, la labor de iniciar con la protección de los activos TI solo constituye una primera, pero, importante fase de una decisión estratégica fundamentada en la exposición y el perfil de riesgo cibernético actual de la industria. Una razón para este proceder, que sin duda hubiese sido el ideal, pero, limitado por el alcance metodológico establecido en esta investigación y circunscrito a los sistemas TI, estriba en que, mientras los entornos de OT suelen estar protegidos por capas de aislamiento físico o protocolos propietarios menos expuestos a la red pública, los activos TI constituyen la superficie de ataque primaria y más vulnerable, sirviendo frecuentemente como la puerta de entrada para amenazas que, luego, intentan escalar hacia la infraestructura OT .

Desarrollar en esta tesis la protección de los sistemas TI asociados a la cadena de producción del sector flexográfico, postergando la labor de completar el modelo cibernético protectivo con la integración profunda de OT para un trabajo futuro, permitirá establecer de manera inicial, un marco preliminar de protección en las empresas, lo cual facilitará que, cuando se aborden las particularidades de la ciberdefensa de los sistemas OT, se haga sobre una base de gobernanza más sólida, evitando la complejidad técnica de intentar asegurar ambos ecosistemas simultáneamente sin los recursos técnicos, financieros y humanos o sin una adecuada cultura organizacional en el tema de la ciberseguridad.

Con lo anteriormente expuesto, culmina el marco teórico y la revisión del estado del arte, haciendo notar que, por brevedad, se omitieron trabajos investigativos tanto de maestría como de doctorado, también, muy interesantes todos, habiendo tenido que efectuarse una selección, apenas justa y precisa, de lo más granado y representativo, acorde con los objetivos trazados y el interés general de complimentar, adecuadamente, con el propósito de esta tesis de maestría en seguridad informática.

3. Metodología

La metodología es un componente esencial de cualquier trabajo de investigación y cobra particular importancia en el caso de una tesis de maestría en seguridad informática, ya que proporciona el marco estructurado y sistemático que guía todo el proceso de investigación propiamente dicho. El método articula, desde la identificación del problema hasta la validación de los resultados y, en este sentido, una metodología bien definida permite asegurar la rigurosidad científica, la replicabilidad de los procedimientos y la validez de las conclusiones, como se infiere de los lineamientos de [57] y [58].

De esta manera, la metodología de investigación facilitó, la selección adecuada de herramientas, el uso técnicas apropiadas y de procedimientos idóneos para guiar el trabajo exploratorio en búsqueda de la solución deseada. En este sentido, donde las soluciones deben ser, tanto técnicamente sólidas, como aplicables en entornos reales, la metodología se convirtió en el eje garante de la coherencia y la credibilidad técnica del trabajo investigativo. Adicionalmente, y más importante, el método fue la fuente generadora de innovación que constituye valor agregado desarrollado en esta tesis de maestría en seguridad informática y, que se presentará más adelante al igual que, también, la metodología fundamental en los trabajos de [12], [13], [14], [23], [24], [40] [54] y [55] analizados en el estado del arte del capítulo anterior.

En este punto, y para efectos de aclaración metodológica, es importante mencionar que, por razones de tiempo de desarrollo, se estableció acotar el alcance de la presente tesis de maestría en seguridad informática, exclusivamente a la protección de la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica, sin incluir los sistemas OT. Lo anterior, en razón a que los autores cursaron el programa de posgrado de maestría en seguridad informática por vía de transferencia externa (homologación institucional) desde la especialización en ciberseguridad, motivo por el cual, solo se dispuso de diez (10) meses (febrero a noviembre de 2025) para realizar y culminar el

trabajo de investigación y no de los habituales veinticuatro (24) meses con que se cuenta para este propósito y que tiene por duración el programa de posgrado.

3.1 Metodología de investigación

En el presente apartado se exponen los detalles y procedimientos de la metodología utilizada y mediante la cual se desarrollaron y se obtuvieron los resultados y productos de esta tesis de maestría. Al efecto, de manera inicial, se desarrollaron todas y cada una de las actividades descritas, más adelante, en el marco lógico del proyecto, lo cual se soportó en los objetivos generales y específicos para lograr la obtención de los resultados y productos que se esperaban.

3.1.1 Enfoque y tipo de investigación

La presente investigación, acorde con [57], es de carácter mixto porque articula la rigurosidad de la recolección de datos numéricos y métricas de desempeño con la interpretación cualitativa de los usuarios. Por un lado, posee un componente cuantitativo crítico al desarrollar una Prueba de Concepto (PoC), donde la validez se sustenta en resultados que fueron medidos (efectividad, eficacia, reducción del nivel de riesgo cibernético y demás aspectos importantes de los sistemas TI asociados a la gestión OT).

Por otro lado, integra una dimensión cualitativa al emplear instrumentos metodológicos (encuesta de diagnóstico y encuesta de verificación) para validar la relevancia, pertinencia y aplicabilidad del modelo de ciberseguridad propuesto para la infraestructura TI asociada a la cadena y procesos productivos críticos del sector industrial bajo estudio. Esta combinación permite que se pueda demostrar, no solo la utilidad y aplicabilidad del modelo prototipo cibernético protectivo y su funcionamiento técnico, sino que, también, revela que contribuye y es factible de implementar dentro de una PYME del sector objeto de análisis o de una estructura organizacional similar de la economía real que cuente con procesos críticos gestionados por tecnologías TI.

3.1.2 Fases de la investigación

Acorde a los lineamientos de [57], en la Fig. 7, se presenta, en todo detalle, las fases de la metodología diseñada, adoptada e implementada para la realización de la presente investigación y que presenta en detalle el método “step by step”. Al efecto, y como se aprecia, en el método utilizado, y que se consolida en el marco lógico (ver Tabla 1), se aprecian, en detalla, las fases y actividades seguidas y desarrolladas para el cumplimiento de los objetivos generales y específicos a cumplir en para el desarrollo y culminación de esta tesis de maestría en seguridad informática.

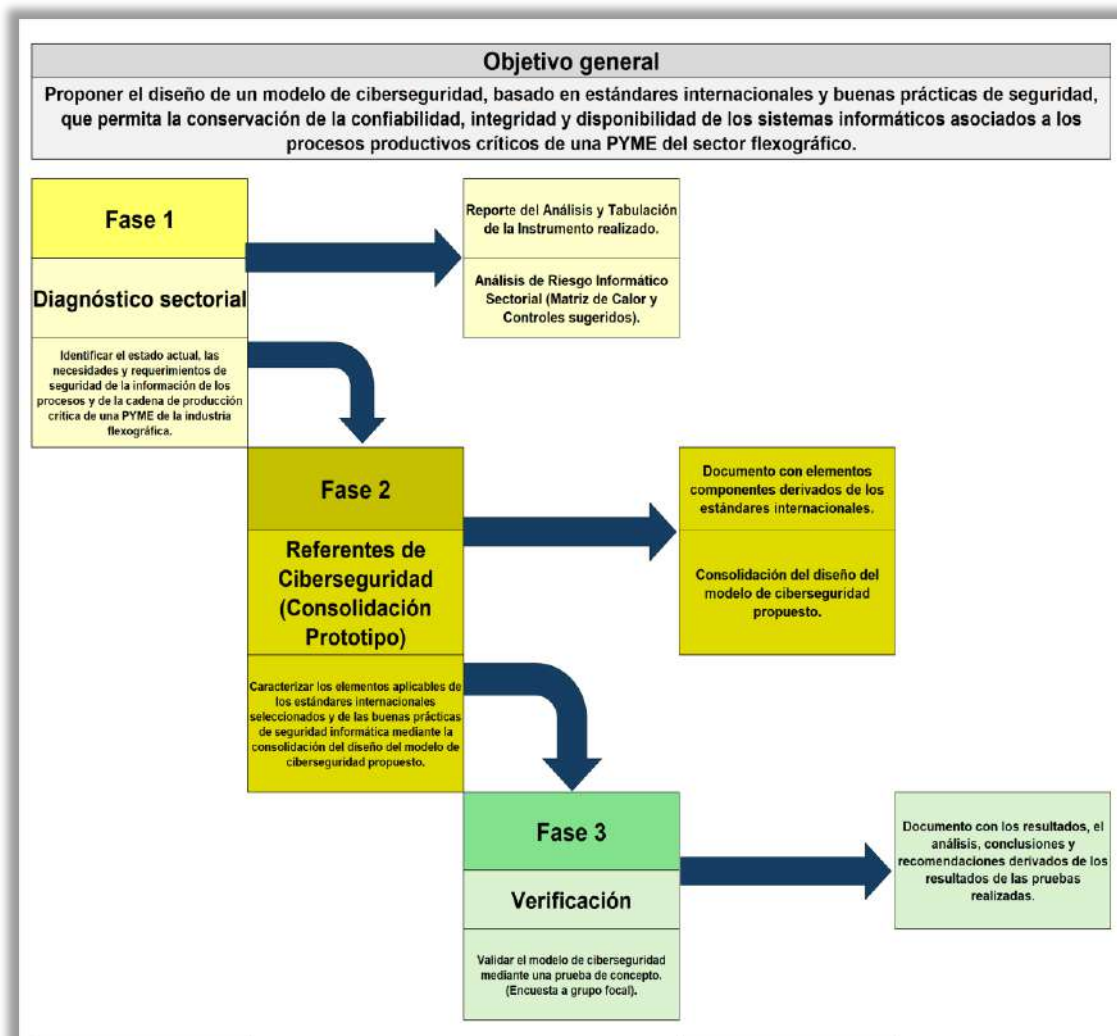


Fig. 7 Fases metodológicas aplicadas para el desarrollo y solución de esta tesis de maestría.

Nota: Fases de la metodología de investigación aplicada para el desarrollo y solución de esta tesis de maestría. Fuente: Autoría propia.

3.2 Marco lógico

Tabla 1. Marco lógico.

Fases	Nombre de la Fase	Objetivo Específico	Actividades	¿Cómo se lograría la actividad?	Entregables
FASE 1	Diagnóstico Sectorial	Identificar el estado actual, las necesidades y requerimientos de seguridad de la información de los procesos y de la cadena de producción crítica de una PYME de la industria	Se estructurará y se aplicará el instrumento a la población objetivo.	Encuesta sectorial real que permita evaluar el estado actual de la ciberseguridad y las necesidades y requisitos de seguridad informática sectorial.	Reporte del Análisis y Tabulación de la Instrumento realizado.
				Elaboración de una Matriz de Riesgo Informático (MRI) acorde al estado general actual de los sistemas informáticos del sector.	Análisis de Riesgo Informático Sectorial (Matriz de Calor).
FASE 2	Revisión de estándares internacionales y consolidación del prototipo de ciberseguridad	Caracterizar los elementos aplicables de los estándares internacionales seleccionados y de las buenas prácticas de seguridad informática mediante la consolidación del diseño del modelo de ciberseguridad propuesto.	Se analizarán los estándares internacionales y se seleccionarán los elementos aplicables al diseño del modelo de ciberseguridad acorde al estado actual de la ciberseguridad y las necesidades sectoriales en seguridad informática. Se conceptualizará y se consolidará el diseño del prototipo de ciberseguridad buscado.	ISO 27001 - Revisión y selección de elementos aplicables	Documento con elementos componentes derivados de los estándares internacionales y mejores prácticas de seguridad aplicables (Controles sugeridos) y consolidación del diseño del modelo de ciberseguridad propuesto.
				ISO 27002 - Revisión y selección de elementos aplicables	
				ISO 22301 - Revisión y selección de elementos aplicables	
				ISO 22361 - Revisión y selección de elementos aplicables	
				ISO 22316 - Revisión y selección de elementos aplicables	
				NIST 2.0 CSF - Revisión y selección de elementos aplicables	
				CIS Controls - Revisión y selección de elementos aplicables	
				Buenas Prácticas de Seguridad Informática - Revisión y selección de elementos aplicables	
				Diseño conceptual del prototipo de ciberseguridad	
				Desarrollo y elaboración del diseño del prototipo de ciberseguridad.	
FASE 3	Verificación	Validar el modelo de ciberseguridad mediante una prueba de concepto	Se definirán los mecanismo de prueba	Definición de la prueba de concepto para probar el modelo de ciberseguridad propuesto.	Documento con los resultados, el análisis, conclusiones y recomendaciones derivados de los resultados de las pruebas realizadas.
			Se realizarán las pruebas	Ejecución de las pruebas acorde a la metodología propuesta para verificar el modelo de ciberseguridad dentro del alcance del proyecto realizado.	
			Se analizarán los resultados	Análisis de los resultados obtenidos y conclusiones sobre el modelo de ciberseguridad dentro del alcance del proyecto realizado.	

Nota. Marco lógico con fases metodológicas de investigación y actividades y entregables asociados al cumplimiento de los objetivos general y específicos de esta tesis de maestría. Fuente: Autoría propia.

El desarrollo del marco lógico mostrado en la Tabla 1 se basó en la metodología por fases (step by step) anteriormente referenciada y diseñada para proporcionar una guía sistemática que condujese al cumplimiento de los objetivos establecidos de protección de la infraestructura TI asociada a la gestión de los sistemas OT de la cadena productiva crítica sectorial, mediante la alineación de actividades, estándares internacionales y el marco CCCI. Esta herramienta metodológica no solo facilitó la planificación y ejecución de la investigación, sino que permitió integrar de manera coherente recursos, procesos y productos finales para diseñar estratégicamente un modelo de ciberseguridad robusto destinado a la infraestructura crítica de la industria flexográfica.

Al efecto, y como se puede observar en la Tabla 1, que presenta el marco lógico, se puede visualizar la relación directa entre los recursos, los procesos, los procedimientos, las acciones, las herramientas, los objetivos, tanto generales como específicos, y los productos esperados (entregables) y a lograr, permitiendo un seguimiento efectivo del progreso investigativo desarrollado en esta tesis de maestría y cuya finalidad fue diseñar un modelo de ciberseguridad para la infraestructura informática y computacional asociada a la gestión, operación y control de la cadena de producción crítica de la industria flexográfica.

En este punto, hay que resaltar que, acorde a los lineamientos de [57] y [58], con el desarrollo metodológico planteado en el marco lógico de la Tabla 1, se logró que la solución de protección propuesta, es decir, el prototipo de ciberseguridad desarrollado, se revelara especialmente adecuado para el contexto de las PYMEs, lo cual exigió la aplicación de un enfoque metodológico de naturaleza sistemática, sistémica y holística muy detallado y que permitiese evaluar las vulnerabilidades y riesgos específicos de la infraestructura TI en las PYMEs y empresas del sector flexográfico, mientras que, simultáneamente, fuese elemento básico para el diseño del modelo de ciberseguridad.

Este desarrollo se realizó bajo los preceptos de defensa en profundidad planteados por [15] y [16], según los cuales se debe establecer una línea base fundamental que, dictaminada por los controles propuestos (encontrados como producto de la revisión de estándares de seguridad informática en la fase 2 y disponibles en el Anexo Nro. 5), facilitó la creación de un prototipo cibernético de seguridad informática robusto, pero, a la vez,

práctico, flexible y adaptable a las necesidades de continuidad y resiliencia operativa de una industria esencial, como lo es la flexográfica.

3.3 Desarrollo del marco lógico

En el contexto de desarrollo del marco lógico se observó como la metodología por fases proporcionó una estructura lógica y secuencial que, permitió ir guiando y abordar de manera organizada, gradual y sistemática las diversas etapas necesarias para consolidar el diseño del modelo de ciberseguridad buscado, que se presenta en [23], [24] y [49] y que será desglosado en todo detalle en el capítulo 4 de resultados de esta tesis de maestría en seguridad informática. Al efecto, el desarrollo del marco lógico, acorde a las recomendaciones de [57], inició por la obtención de la información básica necesaria (diagnóstico sectorial del estado y necesidades de ciberseguridad de la industria flexográfica), pasando por la implementación del prototipo de ciberseguridad basado en el análisis de riesgo informático efectuado, hasta su ajuste y posterior validación mediante la aplicación de un mecanismo de verificación y de validación.

La prueba conceptual, fue efectuada mediante la aplicación de un instrumento (encuesta de verificación del modelo de ciberseguridad) que fue aplicado a las mismas empresas indagadas inicialmente y que dieron base al establecimiento del diagnóstico sectorial de seguridad de la información. Este mecanismo de validación se eligió por su conveniencia metodológica y práctica y, a efectos de lograr la estimación de la mitigación del nivel de riesgo lograda por el prototipo cibernético de protección desarrollado. Esta forma de desarrollo del marco lógico permitió obtener los resultados esperados. Los resultados obtenidos en esta fase se pueden observar en el capítulo de resultados (fase 1) y en los Anexos Nros. 1, 2, 3 y 4.

Finalmente, el desarrollo del marco lógico culminó con la realización de la tercera y última fase, igualmente fundamental en el desarrollo de esta tesis de maestría, pues se trata de una etapa conclusiva clave a efectos del cumplimiento del objetivo general que guio el desarrollo de este trabajo investigativo y que consistió en efectuar la validación y ajuste del modelo de ciberseguridad consolidado y propuesto para la protección de la triada de la CIA

de la infraestructura informática asociada a la cadena de producción de la industria flexográfica. Para esta fase final, se desarrollaron tres (3) actividades, a saber:

- Una primera actividad de definición del mecanismo de prueba conceptual pertinente, encontrándose que una encuesta de verificación bajo los lineamientos de [57] y [58], resultó adecuada teniendo en consideración y como base, las principales métricas del instrumento aplicado en la fase 1, a fin de poder realizar un comparativo que permitiese comparar resultados y estimar el nivel de mitigación y reducción de riesgo cibernético que logra el modelo de ciberseguridad propuesto.
- Una segunda actividad, de realización de la encuesta de verificación, y
- Una tercera y final actividad de análisis de resultados y ajuste fino del prototipo realizada con base en los resultados arrojados por la aplicación del instrumento utilizado para la realización de la prueba conceptual.

Al efecto, con la realización de todas las actividades de esta tercera y final fase investigativa, se logró el cumplimiento del tercer objetivo específico trazado, comprobando y constatando la idoneidad del modelo de ciberseguridad propuesto. Verificación que también, puede complementarse con las contribuciones realizadas en [23], [24] y [49] (ver Anexos Nros. 13 y 14) con los varios productos derivados de esta tesis de maestría en seguridad informática. De otra parte, sobre los aspectos metodológicos aplicados, la Fig. 8 muestra el esquema general completo de la estructura metodológica desarrollada en esta tesis de maestría. Como se aprecia, la estructuración metodológica parte de la pregunta de investigación, la cual se consolida en un objetivo general a cumplir y que se desglosa en tres (3) objetivos específicos, cada uno de ellos alineado con una fase metodológica y unas actividades que fueron realizadas.

Adicionalmente, se presentan los intentos de varios modelos que requirieron ser modificados y mejorados (color rojo) derivando en la consolidación del prototipo cibernético protectivo final y que permitieron lograr la meta final trazada de protección y defensa de la triada de la CIA con el modelo de ciberseguridad propuesto. Similarmente, también, se presentan la alineación de los productos de investigación derivados del desarrollo investigativo de esta tesis de maestría. Como el esquema estructural del método seguido

4. Resultados

4.1 Resultados de la fase 1 respecto al diagnóstico del estado, necesidades y requerimientos de seguridad de la infraestructura TI asociada a la cadena de producción de la industria flexográfica

Como se presentó en el desarrollo del marco lógico y según las directivas de [55], la aplicación del instrumento inicial (encuesta de “Diagnóstico del estado actual de la seguridad de la información en el sector flexográfico”) posibilitó la obtención de los resultados de la fase 1 de esta tesis de maestría, pues, con base en la tabulación y análisis de los resultados obtenidos de la encuesta, se logró tanto la identificación del estado actual, las necesidades y requerimientos de seguridad de la información de la infraestructura informática asociada a la gestión de la cadena de producción crítica de las PYMEs y empresas de la industria flexográfica, como, también, la consolidación del análisis y la evaluación del riesgo que se presentan en la respectiva matriz de riesgo y su mapa de calor en el Anexo Nro. 4 de esta tesis de maestría.

Antes de presentar los resultados obtenidos, vale apuntar que, tanto durante la realización de la fase 1, de diagnóstico sectorial, como, también, durante la ejecución de la fase 3, de verificación del modelo de ciberseguridad, se informó y se explicó con claridad, a las empresas encuestadas, que por razones de alcance metodológico, el trabajo de tesis estaba acotado a la infraestructura TI, sin incluir las tecnologías OT, las cuales estaban destinadas a un trabajo de investigación futuro que completara el presente esfuerzo investigativo. De tal manera que los resultados y hallazgos, deben interpretarse en dicho contexto, sin que pierdan validez alguna en su propio ámbito de aplicación y dominio, i.e., sistemas TI.

4.1.1 Resultados de la actividad 1.1 de la fase 1

4.1.1.1. Aspectos metodológicos de la aplicación del instrumento.

4.1.1.1.1. Universo, marco muestral y población objetivo.

La Tabla 2, a continuación, muestra la composición de empresas de la industria flexográfica encuestadas al azar por método probabilístico derivado de la selección al azar de compañías de la base de datos general de clientes de la empresa Serviflex Arco Internacional S.A.S., a saber:

Tabla 2. Marco muestral de aplicación del instrumento metodológico de diagnóstico inicial.

TAMAÑO EMPRESARIAL						
MICROS	PYMES	MEDIANAS	GRANDES	Total Empresas Encuestadas	NO RESPONDIERON	TOTAL
1	13	7	4	25	5	30
4%	52%	28%	16%	100%		
ACTIVIDAD EMPRESARIAL PRODUCTIVA				POBLACIÓN ESTIMADA TOTAL INDUSTRIA FLEXOGRÁFICA		
EMPAQUES FLEXIBLES	ETIQUETAS	CARTÓN CORRUGADO	TOTAL ENCUESTAS			
16	9	0	25			
64%	36%	0%	100%			
TAMAÑO DE MUESTRA		Cantidad	OBSERVACIONES			
No respondieron		5	Cartón Corrugado			
Respondieron		25	Empaques Flexibles y Etiquetas			
TOTAL ENCUESTAS		30	Total Industria Flexográfica			
TAMAÑO POBLACIÓN		176	PORCENTAJE (%) POBLACIÓN		100%	
TAMAÑO MUESTRA		30	PORCENTAJE (%) MUESTRA		17%	

Nota: Marco muestral de aplicación del instrumento metodológico de diagnóstico sectorial (ver Anexo Nro. 2).

Fuente: Autoría propia.

4.1.1.1.2. Población y selección muestral

La selección de la muestra se basó en una población o universo de ciento setenta y seis (176) empresas registradas en la base de datos corporativa, sobre la cual se realizó un muestreo probabilístico aleatorio simple, garantizando que todos los

sujetos de la población objetivo (empresas de flexografía) tuvieran la misma probabilidad de ser incluidos. Para asegurar la transparencia y el rigor estadístico, la elección se realizó mediante un generador de números aleatorios aplicado al censo total de la base de datos, lo que permitió minimizar el sesgo de selección y fortalecer la validez de los resultados obtenidos para el diseño del modelo de ciberseguridad de la infraestructura TI vinculada con la cadena de producción crítica sectorial. De esta manera el sector encuentra representatividad en la aplicación realizada del instrumento metodológico.

4.1.1.1.3 Representatividad y tamaño muestral

Basados en el Teorema del Límite Central, se seleccionó una muestra de treinta (30) empresas ($n=30$), mediante muestreo aleatorio simple, en razón a que esta cantidad es considerada estadísticamente, como el tamaño de muestra mínimo para que la distribución de los datos empiece a aproximarse a una distribución normal. Aunque el tamaño muestras representa el 16,8% de la población total, se considera una muestra significativa y válida para los propósitos de este diseño de modelo de ciberseguridad para la infraestructura TI vinculada a la cadena de producción crítica sectorial, pues, cumple con el tamaño mínimo sugerido por [57], [58] y por la literatura estadística para el análisis de tendencias y permitiendo un manejo profundo de las variables críticas en la infraestructura informática evaluada.

4.1.1.2 Tabulación de resultados del instrumento aplicado

A continuación, en la Tabla 3, se observa un resumen de las preguntas del instrumento metodológico aplicado para la obtención del diagnóstico inicial del estado y requerimientos de la seguridad de la información sectorial, el cual fue efectuado acorde a los preceptos y lineamientos metodológicos de [57] y [58], a fin de garantizar una indagación idónea, sobre todos los pormenores y la realidad de la industria flexográfica en cuanto a su estado actual, sus necesidades y requerimientos de ciberseguridad para la infraestructura IT asociada a la gestión, operación y control de su cadena de producción esencial. Adicionalmente, y para mayor detalle, el instrumento aplicado, en su versión completa, puede observarse en el Anexo Nro. 1.

Tabla 3. Encuesta de diagnóstico de estado y necesidades de seguridad de la información del sector flexográfico. Resumen.

PREGUNTA NRO.	CUESTIONAMIENTO / PREGUNTA
1	¿Su empresa cuenta con una estrategia, plan o protocolo de ciberseguridad o de manejo de incidentes cibernéticos, formalmente implementado, que asegure la confiabilidad, integridad y disponibilidad de sus sistemas y equipos informáticos, en especial los de su cadena de producción?
2	¿Su empresa tiene formalmente implementadas medidas de seguridad, como antivirus o antimalware licenciados , para proteger los sistemas informáticos y la información corporativa contra amenazas maliciosas, como ataques cibernéticos?
3	¿Su empresa cuenta con personal o un departamento de ciberseguridad que asegure la confiabilidad, integridad y disponibilidad de su infraestructura y equipos informáticos, en especial los de su cadena de producción?
4	¿Existen controles, como contraseñas seguras con factor de doble autenticación (2FA) , en los equipos informáticos de gestión y operación de la producción que restringen el acceso a personal no autorizado?
5	¿Los empleados, incluido el personal de planta y de producción, reciben capacitación regular y periódica sobre buenas prácticas de seguridad informática?
6	¿La empresa tiene un sistema de respaldo (copias de seguridad o Backups) , ya sea físico o en la nube, de su información crítica, en especial la de su cadena de producción?
7	¿La empresa evalúa y analiza de manera formal, regular y periódica, el nivel de riesgo cibernético asociado con la seguridad informática de sus equipos, sistemas y dispositivos informáticos, en especial de aquellos que están asociados a la gestión y operación de los procesos de producción?
8	¿Existe en su empresa un compromiso directivo y de la alta gerencia con respecto a la seguridad informática y la ciberseguridad de la organización?
9	¿Su empresa cuenta con maquinaria o equipos de su línea de producción que tengan conexión eventual, temporal o permanente a internet o a otras redes , ya sean internas (LAN – Red corporativa, como la del área de calidad, mantenimiento, etc.) o externas (proveedores, fabricantes, clientes, etc.)?
10	¿Ha sufrido su empresa incidentes o ataques informáticos en el pasado?
11	Utiliza un equipo computacional viejo y obsoleto en su cadena de producción?
12	¿Qué sistema operativo utiliza(n) su(s) equipo(s) computacional(es) asociados a la gestión de su cadena de producción?

Nota: Resumen de las preguntas efectuadas en la encuesta sectorial (ver Anexo Nro. 1). Fuente: Autoría propia.

A continuación, en la Tabla Nro. 4, se observa un resumen de los consolidados derivados de la tabulación realizada de los resultados obtenidos de la aplicación del instrumento metodológico inicial a la población objetivo (encuesta de “Diagnóstico del estado actual de la seguridad de la información en el sector flexográfico”), la cual, se puede observar en mayor detalle en el Anexo Nro. 2 de esta tesis de maestría (archivo Excel). Es de notar que, en la Tabla Nro. 4 se registran los aspectos más relevantes encontrados con la aplicación del instrumento, a saber:

Tabla 4. Tabulación de resultados de encuesta de diagnóstico de estado y requerimientos de seguridad de la información en la infraestructura TI asociada a la cadena productiva crítica del sector flexográfico colombiano (2025).

PREGUNTA NRO.	OPCIÓN DE RESPUESTA (Escala de Likert)					
	0	1	2	3	4	5
1	15	3	1	0	2	4
2	1	4	10	3	2	5
3	6	6	5	1	4	3
4	2	2	13	0	2	6
5	15	5	0	2	1	2
6	0	1	6	4	6	8
7	9	5	4	0	5	2
8	2	7	7	1	2	6
9	3	8	5	0	4	5
10	4	0	0	0	0	21
11	3	3	7	2	7	3
12	Sistemas operativos identificados					
	Win XP	0		Win 11	17	
	Win 7	11		Linux	0	
	Win8	0		MacOS	0	
	Win 10	18				

Nota: Tabulación de resultados de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Estos mismos resultados se pueden apreciar en más detalle y completitud en el formato Excel del Anexo Nro. 2 adjunto a este informe de tesis de maestría. Fuente: Autoría propia.

Consecuentemente y producto del análisis estadístico de los resultados obtenidos y como se observa, más adelante, en la Fig. 12, se muestran los resultados generales obtenidos en la encuesta diagnóstica aplicada a empresas del sector flexográfico, con el objetivo de establecer el estado actual de la seguridad de la información y así identificar las brechas relevantes (destacadas en color rojo, naranjado y amarillo) a fin de realizar el análisis y la evaluación del riesgo informático (matriz de riesgo y mapa de calor) necesarios para la selección de controles y elementos que permitan la consolidación del diseño de un modelo de ciberseguridad apropiado. Un análisis conceptual más completo se puede observar en el Anexo Nro. 2, formato PDF, adjunto al final de esta tesis de maestría.

En resumen, los resultados evidencian una preocupante falta de madurez en la gestión de la seguridad informática en los sistemas TI asociados a la gestión de las cadenas productivas críticas del sector. Por ejemplo, en la pregunta P1 (“Estrategia y plan proactivo de ciberseguridad”), Quince (15) respuestas se ubican en el nivel más bajo (valor 0), lo cual indica la ausencia de políticas o estrategias de ciberseguridad claramente establecidas. Este patrón se repite en la P6 (“Respuesta a incidentes de seguridad o fuga de información”), donde Quince (15) respuestas también indican la inexistencia de mecanismos de respuesta. Del mismo modo, en P3 (“Personal a cargo de la ciberseguridad”), la mayoría (13) manifestó niveles muy bajos (valor 1), lo que sugiere la falta de designación de roles o responsables en esta área crítica.

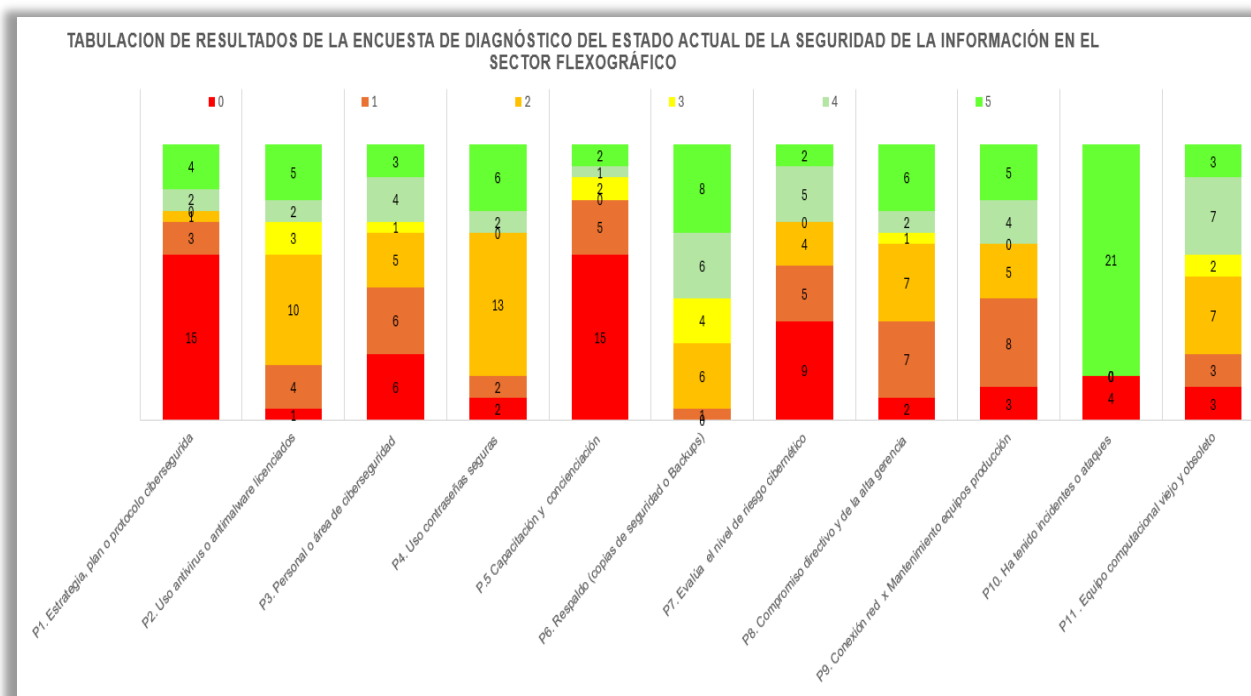


Fig. 9 Gráfico de resultados por pregunta obtenidos en diagnóstico de estado y requerimientos de seguridad de la información en sector flexográfico 2025.

Nota: Estos resultados se pueden apreciar en más detalle en el Anexo Nro. 2, archivo en formato Excel adjunto a esta tesis de maestría. Fuente: Tomado de: Autoría propia.

En contraste, se observan indicadores más positivos en preguntas como P10 (“Ha habido incidentes o ataques”), donde Veintiún (21) respuestas se ubican en nivel 4, lo que puede interpretarse como una mayor conciencia producto de experiencias previas. No obstante, este dato también puede interpretarse como una alta exposición a riesgos que no han sido debidamente gestionados, dada la debilidad en los otros dominios.

Asimismo, en las preguntas P5 (“Capacitación y concienciación”) y P9 (“Conectividad + Mantenimiento equipo producción”), se evidencian algunos niveles medios y altos (valores 3, 4 y 5), aunque siguen predominando los niveles bajos, lo cual indica esfuerzos aislados y no sistemáticos.

En conclusión, este análisis cuantitativo preliminar respalda la necesidad urgente de implementar un modelo de ciberseguridad adaptado a las condiciones de las PYMEs del sector flexográfico, que contemple desde la planeación estratégica hasta la respuesta a incidentes, y que promueva una cultura organizacional basada en la gestión proactiva de riesgos. Esta información fue el insumo clave y la base para el diseño ingenieril de un modelo de ciberseguridad bien sustentado y apuntalado en controles apropiados, extractados de los estándares internacionales y de las buenas prácticas de seguridad informática, como el caso del prototipo cibernético de defensa propuesto y objeto de investigación en esta tesis de maestría.

De otra parte, el gráfico de Pareto, que se observa en la Fig. 10, clasifica los aspectos más críticos de la seguridad de la información en las infraestructuras TI asociadas a la cadena de producción crítica de las empresas del sector flexográfico, en función de las respuestas que obtuvieron un nivel “0”, es decir, la ausencia total de implementación o control en ese aspecto específico de ciberseguridad. Esta visualización permitió priorizar las intervenciones correctivas desde una perspectiva estratégica y orientada al cierre de brechas de seguridad, y fueron insumo de consideración en el diseño del modelo de ciberseguridad propuesto y aplicable al sector flexográfico (aun cuando se reveló su potencialidad de aplicación para otras industrias similares con cadenas productivas esenciales y críticas). Los dos (2) aspectos más críticos (**Px**: pregunta Nro.), con Quince (15) ocurrencias cada uno, son:

- **P1**: Estrategia, plan o protocolo de ciberseguridad, y
- **P5**: Capacitación y concienciación.

Estos resultados indicaron que la mayoría de las empresas no cuentan, ni con una estrategia estructurada de ciberseguridad, ni con programas formativos en dicha

temática para su personal. La ausencia de estos dos (2) pilares compromete no solo la prevención de incidentes, sino, también, la capacidad de respuesta empresarial ante eventualidades cibernéticas o ataques maliciosos y respecto al desarrollo e instauración de una cultura de ciberseguridad fuerte y arraigada al interior de cada organización y empresa del sector, particularmente, en PYMEs.

En tercer lugar, se encuentra P7: Escala el nivel de riesgo cibernético, con Nueve (9) registros en nivel 0, lo que refleja que las organizaciones no realizan análisis de riesgo formalizados. Esto representa un punto crítico, ya que, sin una correcta identificación y evaluación del riesgo, no se pueden asignar controles de forma eficiente. Otros aspectos con alto grado de criticidad incluyen:

- **P3:** Personal a cargo de la ciberseguridad (seis (6) veces en nivel 0),
- **P10:** Ha habido incidentes o ataques (cuatro (4) casos sin ningún tratamiento posterior a la presentación del ciberincidente), y
- **P9 y P11:** Infraestructura técnica y mantenimiento con tres (3) casos cada uno.

Los aspectos menos críticos, aunque no por ello resueltos adecuadamente y, todos, con menos de Tres (3) respuestas en nivel 0, son:

- **P4:** Uso de contraseñas seguras,
- **P8:** Compromiso directivo y de la alta gerencia,
- **P2:** Uso antivirus o antimalware, y
- **P6:** Respaldo (copias de seguridad o backup)

La curva o análisis de Pareto mostrada, a continuación, en la Fig. 10, demuestra que solo tres (3) factores (P1, P5 y P7) representan más del 70% de la criticidad acumulada, lo que sugirió la necesidad de una intervención priorizada y focalizada sobre estos

potenciales aspectos de riesgo, a fin que, mediante el diseño del modelo de ciberseguridad realizado, se logrará tener un impacto significativo y que permitiese una mitigación apreciable e importante del nivel de riesgo informático para las PYMEs y demás compañías del sector flexográfico y, adicionalmente, potenciar la mejora general de la postura de ciberseguridad sectorial.

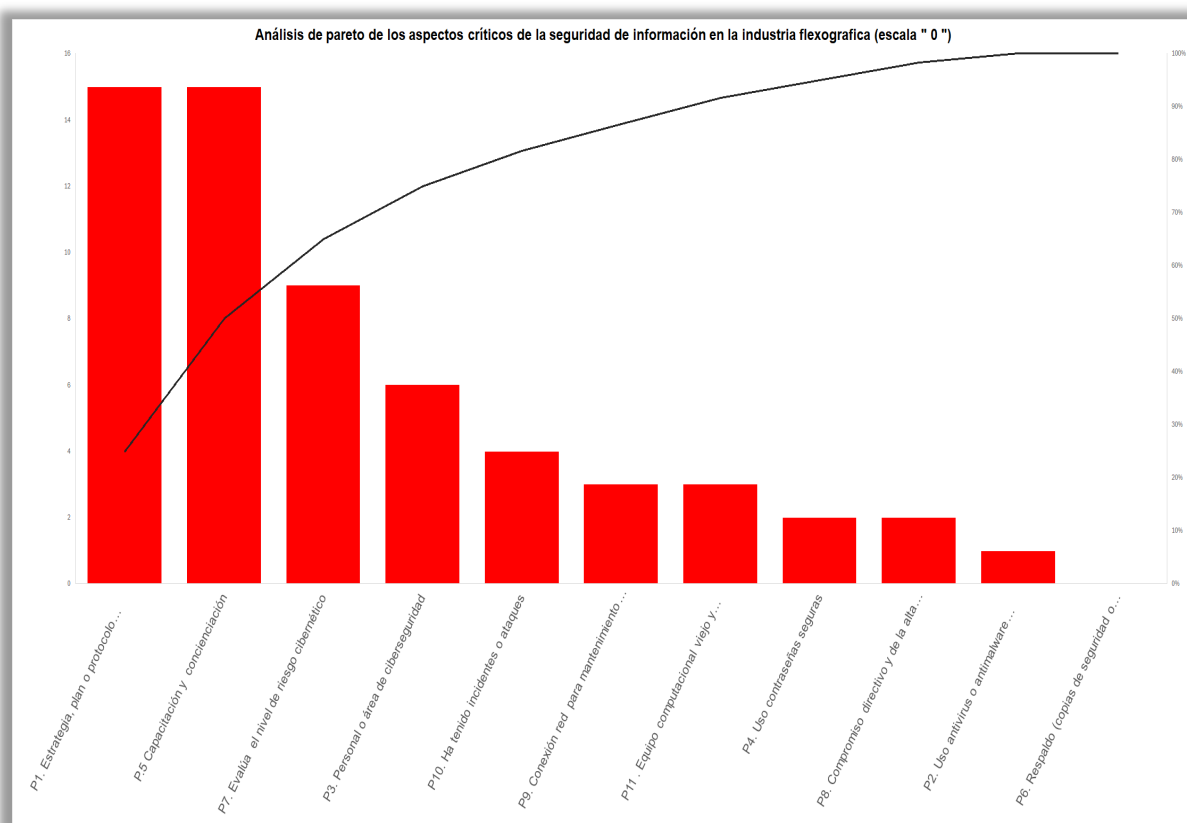


Fig. 2 Análisis de Pareto de los aspectos críticos de ciberseguridad obtenidos en la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico.

Nota: Análisis de Pareto (Escala "Cero" (0)) de los aspectos críticos de ciberseguridad obtenidos en la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico colombiano 2025. Fuente: Tomado de: Autoría propia.

En síntesis, el análisis de Pareto, realizado bajo las directivas de [18], confirmó la hipótesis central de esta investigación de maestría: el sector flexográfico colombiano requería, con urgencia, de un modelo de ciberseguridad efectivo, eficaz, adaptado, escalable y pedagógicamente accesible, que atendiese, en primera instancia, la ausencia de planeación estratégica, la falta de programas de capacitación, y la no evaluación del riesgo cibernético, como focos fundamentales para lograr la protección de una infraestructura digital que asegure la continuidad y la resiliencia de las cadenas productivas críticas y esenciales del sector.

Complementariamente, como se observa, a continuación, en la Tabla 5, otro aspecto importante que fue develado por el análisis de los resultados de la encuesta de diagnóstico del estado y necesidades de la seguridad de la información de la industria flexográfica y que, también, sirvió de insumo para el diseño del modelo de ciberseguridad propuesto en esta tesis, es que, como resultado adicional de procesar la información estadística y conceptual, se construyó la siguiente matriz DOFA donde se reflejaron las debilidades, oportunidades, fortalezas y amenazas que enfrenta el sector flexográfico en cuanto a ciberseguridad y de la cual se efectuó un análisis más detallado y completo que se presenta en el Anexo Nro. 2 de esta tesis de maestría.

Tabla 5. Matriz DOFA elaborada con base en los resultados de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025.

Matriz DOFA – Diagnóstico de Ciberseguridad del Sector Flexográfico 2025	
Fortalezas (F)	Debilidades (D)
F1. Presencia significativa de sistemas de respaldo y copias de seguridad.	D1. Ausencia generalizada de estrategias formales de ciberseguridad e incident response.
F2. Algunas empresas reportan uso de medidas antivirus y antimalware robustas.	D2. Carencia de personal o departamentos especializados en ciberseguridad.
F3. Un grupo reducido de empresas cuenta con compromiso directivo visible.	D3. Falta de implementación de controles de acceso seguros y autenticación multifactor.
F4. Algunas compañías utilizan sistemas operativos actualizados (Windows 10/11).	D4. Casi total ausencia de programas de capacitación y concienciación en ciberseguridad.
	D5. No se realizan análisis periódicos de riesgo cibernético.
	D6. Uso persistente de sistemas operativos obsoletos (Windows 7).
	D7. Alta heterogeneidad en la adopción de prácticas de ciberseguridad básica.
Oportunidades (O)	Amenazas (A)
O1. Incrementar el compromiso directivo mediante sensibilización sobre riesgos.	A1. Alta incidencia de ciberataques previos, incluyendo casos de ransomware con pérdidas significativas.
O2. Disponibilidad de normas y marcos internacionales como NIST, ISO 27001, etc.	A2. Equipos de producción conectados a redes e internet sin protección adecuada.
O3. Posibilidad de formación continua mediante alianzas con entidades académicas.	A3. Obsolescencia tecnológica como superficie de ataque activa.
O4. Modernización de sistemas operativos y migración a tecnologías más seguras.	A4. Entorno de amenazas en evolución constante y creciente sofisticación de los ciberataques.
O5. Aplicación de políticas sectoriales de ciberseguridad con apoyo estatal.	A5. Bajo nivel de cultura de ciberseguridad generalizado en el sector.

Nota: Matriz DOFA derivada de los resultados del diagnóstico del estado y requerimientos de seguridad de la información de la infraestructura TI asociada a la cadena de producción crítica del sector flexográfico colombiano 2025. Para detalles ver Anexo 2. Fuente: Tomado de: Autoría propia.

4.1.2 Resultados de la actividad 1.2 de la fase 1

4.1.2.1 Análisis y evaluación del riesgo informático sectorial (matriz de riesgo informático y mapa de calor).

Los resultados obtenidos de la realización de esta actividad, para la cual se adoptaron, como fundamento metodológico, los preceptos y lineamientos de análisis y evaluación de riesgo informático basados en la normatividad ISO 27001 [3], aprendidos durante el desarrollo de la asignatura de gestión y análisis del riesgo, impartida por [18] y cuyos conocimientos adquiridos durante la especialización en ciberseguridad en la institución, en 2024, permitieron dar cuenta de este propósito adecuadamente. También, se adoptaron las recomendaciones de [22] sobre riesgo informático, derivadas de la asignatura Seminario 4 de la propia maestría en seguridad informática de la institución.

Los resultados obtenidos con base en el desarrollo de la actividad 1.1. de la fase 1 (diagnóstico de seguridad de la información de la infraestructura TI asociada a la cadena productiva crítica del sector flexográfico) bajo las directrices de la norma ISO 27001 [3] y de su anexo A permitieron la adecuada consolidación del análisis y la evaluación del riesgo, todo lo cual, fue debidamente plasmado en el formato de la matriz de riesgo y su respectivo mapa de calor, elaborados para esta tesis de maestría y que pueden observarse en el Anexo Nro. 4 (archivo Excel, .xlsx).

Como resultado de la actividad 1.2 de la fase 1, se consigna la matriz de riesgo y el mapa de calor para la infraestructura TI asociada a la cadena productiva crítica del sector flexográfico, que se presentan en el Anexo Nro. 4 (archivo Excel, .xlsx). Al respecto, vale la pena mencionar que, el formato presentado con la matriz de riesgos y su correspondiente mapa de calor fue compartido por [18], durante la asignatura de gestión y análisis del riesgo en la institución. De otra parte, también, vale mencionar que, muchos diversos tipos formatos, muy similares al utilizado, o con variaciones muy leves, pero, que conservan lo esencial de los lineamientos

para análisis y evaluación de riesgo de la norma ISO 27001 [3], se encuentran disponibles, públicamente, para su acceso y uso, en la internet.

Al efecto, y tal como indicó [25], el método utilizado para la elaboración de la matriz de riesgos se presenta, en resumen, en la Fig. 11. Como se puede apreciar, se partió del proceso de tabular los resultados obtenidos en el instrumento aplicado (encuesta sectorial de diagnóstico inicial de ciberseguridad del sector flexográfico) y de realizar su análisis, para luego, elaborar los diagnósticos o autoevaluaciones.



Fig. 3 Procedimiento de consolidación del resultado obtenido del análisis y la evaluación del riesgo cibernético para la infraestructura TI asociada a la cadena productiva crítica sectorial.

Nota: Procedimiento de consolidación del análisis y la evaluación del riesgo informático para la infraestructura TI asociada a la cadena productiva crítica del sector flexográfico (Fase 1. Actividad 1.2).

A este respecto, se consolidaron, como resultado parcial de esta actividad 1.2, dos (2) diagnósticos que, convergieron hacia los mismos resultados, uno de ellos realizado bajo los lineamientos de la norma ISO 27001 y, el otro, acorde a las recomendaciones del marco NIST 2.0 CSF. Dichas autoevaluaciones sirvieron de insumo para la construcción de la matriz de riesgo cibernético del estado de la seguridad informática en la infraestructura TI asociada a la cadena productiva crítica sectorial, particularmente, en las PYMEs y empresas de la industria flexográfica. Ambas autoevaluaciones y sus resultados se presentan en el Anexo

Nro. 3 de esta tesis de maestría, mientras que la matriz de riesgo consolidada y su respectivo mapa de calor se presentan en el Anexo Nro. 4.

4.1.2.1.1. Metodología ROA de análisis y evaluación del riesgo informático

Acorde con [18] y [25], la metodología ROA (Risk-Oriented Architecture) o arquitectura orientada al riesgo, es un enfoque que integra la gestión de riesgos directamente en el diseño y la estructura de los sistemas de información y que, a diferencia de los métodos tradicionales que analizan el riesgo cibernético como un evento externo, lo trata como una variable intrínseca del diseño arquitectónico del sistema, puesto que, el método ROA se centra en identificar cómo los componentes de una arquitectura contribuyen a la exposición de la superficie de ataque. Los pasos principales de la metodología ROA, grosso modo, incluyen:

- **Identificación de activos:**

Mapeo de los componentes críticos (servidores, estaciones, aplicativos, bases de datos, etc.).

- **Análisis de flujos e interdependencias:**

Consideración de cómo la falla de un componente afecta al resto del sistema.

- **Cuantificación del riesgo informático:**

Asignación de niveles de criticidad de los activos (para el caso de la infraestructura TI) basados en la probabilidad de compromiso y el impacto en el negocio (cadena de producción).

- **Mitigación estructural del riesgo cibernético:**

Implementación de controles (para el caso extraídos de los referentes y estándares considerados) directamente en la arquitectura del sistema (infraestructura TI asociada a la cadena de producción sectorial bajo estudio) para realizar el adecuado tratamiento de los riesgos (mitigar en lo posible y reducir la superficie de ataque).

Dado que el presente trabajo se enfoca en el sector de la flexografía, el método ROA permite priorizar con base en su criticidad, los activos TI asociados a la gestión y soporte de los procesos OT de la cadena de producción crítica del sector, facilitando una ciberdefensa en profundidad coherente para la infraestructura TI analizada en esta tesis de maestría en seguridad informática.

4.1.2.1.2. Identificación de activos

A este propósito, y según indicaciones de [18] y de [25], el primer paso consistió en identificar todos los activos de información relevantes que fueron mencionados por los encuestados en el instrumento aplicado y que fueron organizados por categorías (hardware, software, factor humano e información). Así pues, los activos se clasificaron en las cuatro (4) categorías fundamentales mencionadas, a saber:

- **Hardware:** estaciones de trabajo (PC), servidores base de datos, discos o unidades de almacenamiento físico donde se realiza el respaldo o backup, y las redes corporativas.
- **Software:** sistemas operativos (Windows 7, 10 y 11), programas y aplicaciones corporativas (softwares licenciados), programas utilitarios (funcionamiento de impresoras) y de almacenamiento como aplicativos de bases de datos, antivirus, antimalware, etc.
- **Factor Humano:** personal operativo y de planta, personal de sistemas y TI y personal contratista (externo).
- **Información:** la cual incluye:
 - tanto la información técnica (como las configuraciones y parámetros operativos de las máquinas impresoras flexográficas, los registros de calibración, las formulaciones de las tintas, los datos de control de calidad, entre otros);

-
- como, también, la información de producción (como archivos digitales de diseño, pre prensa, datos de producción, costos, trazabilidad, etc.).

4.1.2.1.3. Metodología y valoración de la criticidad de los activos informáticos

Como se observó en la Fig. 11 con base en la información obtenida de la aplicación de instrumento y de las autoevaluaciones derivadas, se determinó la importancia y criticidad de cada activo en función de la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura TI asociada a la cadena productiva crítica sectorial, para lo cual, se definió la criticidad cibernética de los mismos acorde con la siguiente metodología de valoración de activos con base en su criticidad, a saber:

4.1.2.1.3.1 Método de cálculo de la criticidad intrínseca del activo

Según [18] y [25], en una metodología orientada al riesgo, como la seguida en este trabajo, la valoración del activo se constituye en el multiplicador del riesgo. Se explica mediante la fórmula técnica:

$$\text{Valor}(\mathbf{A}) = f(C, I, D)$$

Donde el valor del activo **A** es una función de su importancia para el proceso de negocio, es decir, de su relevancia para la infraestructura TI. Por ejemplo, y para el caso, un servidor con la información de la cadena de producción tendría una valoración máxima, ya que su fallo dejaría comprometida a la seguridad de toda la cadena de producción.

Este paso es fundamental porque no se puede proteger lo que no se valora. En particular, para esta tesis de maestría, la valoración de activos justifica por qué el modelo de ciberseguridad se enfoca en ciertos aspectos considerados relevantes y no en otros considerados no tan relevantes, de tal manera que se logra la optimización de esfuerzos económicos o técnicos de protección.

4.1.2.1.3.2 Escala de valoración de la criticidad del riesgo

Como se puede observar, a continuación, en la Tabla 6, con base en la información obtenida de la aplicación de instrumento y de las autoevaluaciones derivadas, se determinó la importancia y criticidad de cada activo en función de la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura TI asociada a la cadena productiva crítica sectorial, para lo cual, se definió la criticidad cibernética de los mismos acorde con la siguiente escala, usualmente utilizada para similares efectos de análisis de criticidad y aprendida del curso de análisis de riesgo de [18] y reconfirmada por de [25], y que se muestra, a continuación, en la Tabla 6, a saber: Alto (alto impacto), Medio (medio impacto) y Bajo (bajo impacto).

Tabla 6. Escalas de valoración de la criticidad del riesgo (Fase 1. Actividad 1.2).

Escala de valoración de activos de la información	
ALTO	Alto impacto
MEDIO	Medio Impacto
BAJO	Bajo impacto
Escala de valoración de la criticidad	
CRÍTICO	Activo Crítico
NO CRÍTICO	Activi No Crítico

Nota: Escalas de Valoración de la criticidad del riesgo (Fase 1. Actividad 1.2). Fuente: Autoría propia.

Al respecto, y tal como se observa de la Tabla 6, la escala de valoración de los activos de información es multidimensional respecto a la pérdida, la indisponibilidad o la alteración de datos y se encuentra granulada en tres (3) diversos niveles de impacto de acuerdo, a la gravedad. De otro lado, respecto a la criticidad, la escala de valoración es operacional respecto a si la cadena de producción puede seguir funcionando y operando, o no, sin el activo analizado. En mayor detalle, para la interpretación de la escala, se tiene:

- **Interpretación de la escala de valoración de los Activos**

La escala de valoración de los activos se estructuró en tres (3) niveles (Alto, Medio, Bajo) que miden la magnitud del impacto sobre los objetivos de la organización ante la pérdida de los pilares de la seguridad de la información en la infraestructura TI asociada a la cadena productiva crítica sectorial, i.e., la confidencialidad, la integridad y la disponibilidad (Triada de la CIA). En particular:

- **Impacto Alto:**

Se interpreta como una afectación grave. Un incidente sobre este activo (ej. filtración de datos sensibles o indisponibilidad prolongada) podría causar el colapso de la cadena de producción con pérdidas financieras significativas, sanciones legales severas o un daño irreparable a la reputación de la institución.

- **Impacto Medio:**

El compromiso del activo genera contratiempos operativos o costos económicos moderados que pueden ser absorbidos, aunque requieren una respuesta inmediata para evitar una escalada o el colapso de la cadena de producción.

- **Impacto Bajo:**

La pérdida de seguridad en este activo tiene un efecto mínimo sin comprometer o arriesgar un colapso de la cadena de producción. La operación puede continuar con alternativas manuales y no hay repercusiones financieras, legales o contractuales de relevancia.

- **Interpretación de la escala de valoración de la Criticidad**

Mientras que la escala de valoración de activos mide el grado del daño, la escala de valoración de la criticidad define la naturaleza o importancia del activo dentro de la continuidad de la cadena de producción de una empresa:

- **Crítico:**

Se refiere a activos indispensables. Si este activo falla o es atacado con éxito, de la cadena de producción asociada se detiene y colapsa por completo, pues, se trata de activos que requieren controles de seguridad de alta disponibilidad y un nivel de monitoreo constante.

- **No Crítico:**

Se trata de activos de apoyo o secundarios y su ausencia, o compromiso, no detiene la operación de la cadena de producción de la organización, permitiendo un cierto margen de maniobra más amplio para su recuperación o sustitución.

Al mismo efecto, y para obtener claridad respecto a la valoración de la criticidad de los activos, según lineamientos impartidos por [25], se formularon las siguientes preguntas cerradas (opciones de respuesta de SI o NO) en aras de precisar los niveles de criticidad de los activos. Las preguntas respecto a la seguridad en la infraestructura TI asociada a la cadena productiva crítica sectorial, a saber, fueron las que se allegan: ¿El activo es susceptible de ser atacado?; ¿El activo es vital para el área de producción?; ¿El activo compromete la operación de la infraestructura TI asociada a la cadena de producción?

Simultáneamente, y para cada activo, estas preguntas se respondieron con base en los resultados obtenidos de la actividad 1.1 de la fase 1 (Encuesta de diagnóstico y necesidades de la seguridad de la información de la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica). Dichas preguntas, sugeridas en la plantilla compartida por [18], permitieron establecer la criticidad de los activos y sus respuestas quedaron consignadas y se pueden encontrar en la matriz de riesgo presentada en el Anexo Nro. 4 (archivo excel, .xlsx) en la separata de Anexos, consignada después de este informe de tesis de maestría en seguridad informática.

4.1.2.1.4. Identificación de vulnerabilidades y análisis de amenazas

De otra parte, y para cada activo identificado e incluido en la matriz de riesgo informático y su mapa de calor, se definieron, entre las más relevantes, tres (3) vulnerabilidades y, consecuentemente, tres (3) amenazas, acorde a los preceptos aprendidos de [16], [18], [19] y reconfirmadas por [25] y [26]. Dichas vulnerabilidades y amenazas son, también, parte integral de la matriz de riesgo informático de la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica, presentada en el Anexo Nro. 4 (archivo excel, .xlsx) y tienen por objetivo posibilitar la estimación del nivel de riesgo informático subsecuente en los sistemas TI vinculados a los procesos de producción.

4.1.2.1.5. Identificación y valoración del riesgo

De similar manera, y como se muestra más adelante, en la Tabla 7, para cada activo, se identificaron los riesgos teniendo en cuenta la escala de valoración, probabilidad, impacto y gravedad del riesgo según los preceptos aprendidos de [18] y reconfirmados por [25] y [26]. Luego, se asignaron los valores de probabilidad (Escala de valores entre 1 y 5) que posibilitaron reflejar qué tan probable es que ocurra un determinado riesgo informático.

Las escalas, mostradas a continuación, en la Tabla 7, fueron implementadas según las orientaciones de [18] y reconfirmadas por [25] y [26] y, en esencia, muestran la valoración del riesgo y la probabilidad de su ocurrencia, así como, además, el correspondiente mapa de aceptabilidad del riesgo cibernético, herramientas que constituyen un aspecto fundamental en el proceso de gestión del riesgo y que son utilizadas para clasificar y determinar qué niveles de riesgo son considerados tolerables (aceptables) o inadmisibles por parte de una organización, y cuáles riesgos son prioritarios y requieren tratamiento inmediato.

Tabla 7. Escalas de valoración, probabilidad, impacto, gravedad y aceptabilidad del riesgo informático inicial para la matriz de riesgo cibernético.

Valoración del Riesgo (matriz)				PROBABILIDAD					
PROBABILIDAD (1 a 5)	IMPACTO 1 a 16	PUNTAJES DE PI 1 a 80			1	2	3	4	5
1 - POCO FRECUENTE	1 - INSIGNIFICANTE	1 a 2 • MÍNIMA	IMPACTO	1	1	2	3	4	0
2 - IMPROBABLE	2 - MENOR	3 a 8 • BAJO		2	2	4	6	8	10
3 - POSIBLE	4 - MODERADO	10 a 16 • MEDIO		4	4	8	12	16	20
4 - PROBABLE	8 - IMPORTANTE	20 a 32 • ALTO		8	8	16	24	32	40
5 - CASI SEGURA	16 - GRAVE	40 a 80 • EXTREMO		16	16	32	48	64	80

Mapa de aceptabilidad del riesgo			
Aceptabilidad del Riesgo	Valoración	% Distribución	Total Riesgos
Inadmisible	33 a 80		
Inaceptable	17 a 32		
Tolerable	9 a 16		
Aceptable	3 a 8		
Muy Aceptable	1 a 2		
		100,0	A determinar

Nota: Escalas de valoración, probabilidad, impacto, gravedad y criterios de aceptabilidad del riesgo informático. Fuente: Tomado de: Autoría propia.

Como se observa las escalas presentadas en la Tabla 7 permitieron cuantificar la valoración del riesgo para los sistemas TI vinculados a los procesos de producción, así como, su probabilidad, posible impacto, gravedad y, también, sus criterios de aceptabilidad. Posteriormente, se definió el impacto (con el establecimiento de una puntuación con valores entre 1 y 16) que posibilitaron reflejar que tan grave sería la afectación en caso de su eventual ocurrencia, siendo el valor de 16 en dicha escala, el valor del mayor impacto posible de acaecer. De esta manera, y según los lineamientos de [18], reconfirmados por [25], se procedió a realizar el cálculo del nivel de riesgo de cada activo informático de la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica, tal como sigue en la siguiente formula y como, también, se puede observar en el Anexo Nro. 4 de esta tesis:

$$\text{Nivel de riesgo} = \text{Probabilidad} \times \text{Impacto}$$

Acorde con los lineamientos de [18], los valores superiores a cuarenta (40) se consideraron de riesgo extremo, por lo tanto, se les prestó especial atención, lo cual permitió priorizar los riesgos calculados más relevantes y cruciales y, como se aprecia a continuación, en la Tabla 12 se muestran los resultados obtenidos en el cálculo del riesgo cibernético realizado para el sector bajo estudio. Su análisis revela una evaluación de trece (13) riesgos de ciberseguridad (R1 a R13), donde se destaca que la mayoría de las amenazas detectadas poseen una gravedad crítica, alcanzándose, en algunos casos, puntuaciones máximas de sesenta y cuatro (64) puntos en la escala de valoración, lo cual manifiesta claramente la eventualidad de altos impactos.

Tabla 8. Resultados obtenidos de análisis y la evaluación del riesgo en la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica.

RIESGO	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD (1-5)	IMPACTO 1-16	GRAVEDAD DEL RIESGO (Probabilidad x Impacto)
R1	Infección de equipos, cifrado de datos, pérdida de productividad e información	4	4	16
R2	Secuestro o corrupción de datos críticos, No disponibilidad, manipulación de la información	4	16	64
R3	Robo de datos confidenciales o sensibles, pérdida del respaldo físico y pérdida de la información	3	16	48
R4	Caída de la red, interrupción del negocio, propagación de malware, interceptación de tráfico	3	8	24
R5	Fallos de seguridad por falta de soporte, explotación del malware, interrupción de operaciones	4	4	16
R6	Exposición a ataques dirigidos, robo credenciales, Malware / Ransomware	4	8	32
R7	Escalada de privilegios, fuga de datos, ataques del día cero	4	4	16
R8	Error humano, mal uso del sistema, alteración o manipulación	3	16	48
R9	Exposición de red o sistemas internos, fuga de información, manipulación indebida	5	8	40
R10	Sabotaje, Configuraciones incorrectas o exposición de datos	3	16	48
R11	Riesgo de manipulación o pérdida de control interno, fuga información	3	16	48
R12	Pérdida de información sensible como formulaciones, condiciones de maquina y otras especificaciones	4	16	64
R13	Interrupción de producción por pérdida de datos críticos	4	16	64

Nota: Resultados del cálculo de riesgo (fase 1, act. 1.2). Ver Anexo Nro. 4 para más detalle. Fuente: Autoría propia.

De otra parte, como se aprecia de la Tabla 8, los riesgos con mayor severidad, como el secuestro de datos críticos (R2), la pérdida de especificaciones técnicas (R12) y la interrupción de la producción (R13), presentan una combinación de probabilidad alta e impacto máximo, lo que exige una estrategia de mitigación inmediata y, en especial, a este respecto, es notable que, a pesar de la variedad de las amenazas establecidas (desde errores humanos hasta eventuales sabotajes), la gran mayoría de organizaciones no tengan, aún, políticas y estrategias concretas para una adecuada gestión del riesgo informático y su propia ciberdefensa y protección digital (particularmente de la triada de la CIA, i.e., de la confidencialidad, integridad y disponibilidad de la seguridad de la información de sus cadenas y líneas de producción críticas).

En este contexto, y teniendo en consideración los resultados arrojados por el cálculo del riesgo, se aprecia que, en particular, cada riesgo tiene diversas opciones de tratamiento, como se muestra, a continuación, en la Tabla 9, que presenta, según [21] y acorde a lo sugerido por [18] y [25], una escala con la descripción clara y la respectiva explicación de cómo el riesgo puede afectar al activo y la respectiva acción a tomar para gestionarlo adecuadamente.

Tabla 9. Alternativas u opciones de tratamiento del riesgo informático.

ACCIÓN	NOTAS Y OBSERVACIONES
EVITAR	Urgente. Intervención inmediata. Puede afectar continuidad del negocio. Implementar controles avanzados, revisar políticas. Se pueden suspender procesos, cambiar tecnologías o rediseñar arquitecturas para que el riesgo no exista.
TRANSFERIR	El riesgo puede delegarse parcial o totalmente a un tercero, como contratar seguros, outsourcing, o servicios gestionados de ciberseguridad.
MITIGAR	Se deben aplicar controles técnicos, administrativos o físicos para reducir la probabilidad o el impacto del riesgo. Ejemplo: firewalls, capacitación, actualizaciones.
ACEPTAR	El riesgo es aceptable. Se documenta y monitorea. No se justifica una inversión significativa para reducirlo más.

Nota: Los riesgos encontrados fundamentalmente se trataron con la opción de mitigación buscando, mediante el modelo de ciberseguridad propuesto, reducir significativamente el nivel de riesgo informático inicialmente encontrado. Fuente: Tomado de: Autoría propia.

Como se puede observar, las alternativas de tratamiento estriban entre evitar, transferir, mitigar o convivir con la aceptación del riesgo cibernético. En particular y bajo la consideración del propósito último establecido en esta tesis de maestría a través de su objetivo general y de sus objetivos específicos, el diseño del modelo de ciberseguridad propuesto fue desarrollado para lograr la

reducción y mitigación de los riesgos cibernéticos asegurando una efectiva y eficaz protección de la triada de la CIA de la seguridad de la información para la infraestructura informática de gestión y operación de la cadena de producción crítica de la industria flexográfica, efecto para lo cual, se incluyó la gestión optima de riesgos cibernéticos bajo los lineamientos de la norma ISO 27001 e indicaciones de [18] y [25], reconfirmadas por [26].

4.1.2.1.6. Mapa de calor de la infraestructura TI analizada

El mapa de calor representa de manera gráfica, visual y muy sencilla la priorización de los riesgos más críticos, facilitando sustancialmente el análisis de los riesgos y posibilitando priorizar las acciones de control necesarias en la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica, tal como sugieren [18] y [25]. Como se aprecia en la Fig. 12, el sector flexográfico acusa algunos riesgos cibernéticos muy preocupantes (R2, R12, y R13) y otros inquietantes (R3, R8, R10 y R11), ambos objetos de pronta y urgente atención. También, existen algunos otros riesgos a considerar, pero, de menor relevancia, como (R1, R5, y R7). El mapa de calor del riesgo informático derivado del diagnóstico inicial del estado y necesidades de ciberseguridad del sector flexográfico puede observarse, a continuación, en la Fig. 12. Para mayor detalle y completitud, también, puede apreciarse, en el Anexo Nro. 4 de esta tesis.



Fig. 4. Mapa de calor inicial del riesgo informático en la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica.

Nota: Se muestran los riesgos cibernéticos hallados para los sistemas TI en el diagnóstico sectorial. Para mayor detalle véase Anexo Nro. 4. Fuente: Tomado de: Autoría propia.

4.1.2.1.7. Mapa de aceptabilidad del riesgo para la infraestructura TI analizada

De otra parte, la Tabla 10, implementada según indicaciones de [25], muestra el mapa de aceptabilidad inicial del riesgo informático encontrado inicialmente en la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica, el cual es resultado de la valoración consolidada con base en el análisis de los resultados del instrumento aplicado (encuesta de diagnóstico del estado actual y necesidades de la seguridad de la información en la infraestructura TI asociada a la cadena de producción crítica de la industria bajo estudio) y los criterios de una adecuada gestión del riesgo cibernético. Al respecto, y como se comentó más atrás, el mapa de aceptabilidad del riesgo que se aprecia en la Tabla 10, permitió definir los criterios de priorización para la atención de los riesgos hallados y, consecuentemente, proceder a su pronta mitigación mediante la adecuada selección de los controles más adecuados y convenientes, resultantes de la revisión de los estándares internacionales de seguridad informática ya mencionados y de las buenas prácticas de seguridad.

Tabla 10. Mapa de aceptabilidad inicial del riesgo cibernético para la infraestructura TI analizada

Mapa de aceptabilidad Inicial			
		% Distribución	Total Riesgos
Inaceptable	33 a 80	61.5	8
Tolerable	17 a 32	15.4	2
Aceptable	9 a 16	23.1	3
Muy Aceptable	3 a 8	0.0	0
Admisible	1 a 2	0.0	0
		100.0	13

Nota: El mapa de aceptabilidad del riesgo muestra los criterios de aceptabilidad del riesgo. Para mayor detalle véase Anexo Nro. 4. Fuente: Tomado de: Autoría propia.

4.1.2.1.8. Resumen del estado de la seguridad informática en la infraestructura TI asociada a la cadena de producción del sector flexográfico

Entre los aspectos más significativos encontrados y derivados de los resultados de la encuesta de diagnóstico inicial del estado y requerimientos de la información del sector flexográfico y que contribuyen a incrementar su superficie de ataque y su riesgo ante acciones maliciosas cibercriminales, principalmente, se tienen:

- En general, el sector no cuenta con estrategias de seguridad informática formalmente establecidas, salvo muy contadas excepciones.
- La protección de la infraestructura TI, incluidos sistemas, equipos, servidores, redes, aplicaciones, bases de datos es muy básica, incipientes e, incluso, totalmente inexistente en algunos casos.
- Las empresas no cuentan con políticas de seguridad informática claras, es escasa la sensibilización y la formación del personal en ciberseguridad, no se cuenta con personal especializado de dedicación exclusiva al área de la seguridad informática suscribiendo esta responsabilidad al proveedor externo del servicio de sistemas e informática y no se tiene mayor preocupación por el asunto, y
- es mínima o, en general, nulo el análisis y evaluación de riesgo cibernético y esta circunstancia representa un punto crítico, ya que, sin una correcta identificación y evaluación del riesgo, no se pueden asignar controles de forma eficiente para proteger la infraestructura TI de las empresas.

Mayoritariamente, el sector flexográfico tampoco cuenta con estrategias definidas de continuidad y resiliencia para fortalecer su infraestructura TI, incluidos, suscribiéndose al uso de backups o copias de seguridad como casi único y exclusivo respaldo operacional. Tampoco, existen, en la mayoría de las empresas, estrategias, planes o protocolos de ciberseguridad, ni tampoco

Primero, se definieron los criterios de medición, estableciendo escalas cuantitativas que permitieron valorar, tanto la probabilidad de ocurrencia de un evento, como su consecuente impacto sobre los activos informáticos críticos. Estos criterios junto con las convenciones usadas pueden observarse, a continuación, en la Tabla 11 que, resume las diversas escalas de valoración utilizadas en la matriz de riesgo informático consolidada para la infraestructura TI asociada a la cadena de producción.

En segundo lugar, se calificaron ambas dimensiones en una escala numérica que va de uno (1) a cinco (5), según plantean [16] y [18], dicha escala se acompaña de descriptores cualitativos que orientan la asignación de la valoración, para facilidad de comprensión, aplicación y consolidación. En tercer lugar, se procedió a combinar probabilidad y el impacto en una matriz que refleja los diferentes niveles de riesgo para la infraestructura TI asociada a la cadena crítica de producción sectorial, lo cual se hizo obteniendo el valor resultante de multiplicar ambos factores (probabilidad e impacto), de modo que los riesgos se distribuyen en un rango que permite clasificarlos, categorizados y priorizados desde los más críticos hasta los más bajos.

De manera similar, y tal como recomiendan [16] y [18], para facilitar la interpretación de la matriz de riesgo informático consolidada, los resultados se representan mediante un código de colores, donde los tonos verdes indican riesgos bajos, los amarillos señalan riesgos moderados, los naranjas corresponden a riesgos altos y los tonos rojos a riesgos críticos y que requieren atención inmediata, tal como se puede observar en la Tabla 11, la cual forma parte integral en el aparte de convenciones de la matriz de riesgo cibernético consolidada para la infraestructura TI asociada a la cadena crítica de producción sectorial y cuya metodología de elaboración reconfirmó [25].

De otra parte, también, es menester hacer notar que los niveles de valoración de los activos de información de la matriz de riesgo presentados anteriormente se establecieron con base en la definición conceptual de la triada CIA, compuesta por confidencialidad, integridad y disponibilidad y, que representan

elementos fundamentales de ciberseguridad. Esta estrategia de valoración de activos fue resultado del análisis y revisión de los lineamientos y directrices emanados de la norma ISO 27001 [3], en su calidad de estándar fundamental, internacionalmente reconocido y ampliamente aceptado, de análisis de riesgo para protección de sistemas informáticos.

Adicionalmente, debe recordarse que, según recomienda [25], los niveles de valoración de la criticidad de los activos de información de la matriz de riesgo fundados en la triada CIA (confidencialidad, integridad y disponibilidad) se corresponden y se alinean, literalmente, con los propósitos y metas de protección cibernética, definidos en el objetivo general de esta tesis de maestría, en aras de la defensa y salvaguarda de la infraestructura informática asociada a la gestión, operación y control de la cadena de producción crítica de la industria flexográfica. Este procedimiento, según plantean [16] y [18], convierte a la matriz de riesgos y a su respectivo mapa de calor, en herramientas prácticas de priorización, pues permiten a las organizaciones identificar, con claridad, efectividad y eficacia, qué riesgos deben tratarse, gestionarse y atenderse, de forma urgente, cuáles requieren controles preventivos y cuáles riesgos pueden ser aceptados, monitoreados o, incluso, cuales riesgos cibernéticos pueden ser tolerados.

Tabla 12. Riesgos identificados en la infraestructura TI asociada a la cadena de producción del sector flexográfico como resultado de la elaboración del análisis y evaluación del riesgo informático en la industria flexográfica en 2025 (matriz de riesgo y mapa de calor).

RIESGO	DESCRIPCIÓN DEL RIESGO
R1	Infección de equipos, cifrado de datos, pérdida de productividad e información.
R2	Secuestro o corrupción de datos críticos, No disponibilidad, manipulación de la información.
R3	Robo de datos confidenciales o sensibles, pérdida del respaldo físico y pérdida de la información.
R4	Caída de la red, interrupción del negocio, propagación de malware, interceptación de tráfico.
R5	Fallos de seguridad por falta de soporte, explotación del malware, interrupción de operaciones.
R6	Exposición a ataques dirigidos, robo credenciales, Malware / Ransomware.
R7	Escalada de privilegios, fuga de datos, ataques del día cero.
R8	Error humano, mal uso del sistema, alteración o manipulación
R9	Exposición de red o sistemas internos, fuga de información, manipulación indebida.
R10	Sabotaje, Configuraciones incorrectas o exposición de datos
R11	Riesgo de manipulación o pérdida de control interno, fuga información.
R12	Pérdida de información sensible como formulaciones, condiciones de máquina y otras especificaciones.
R13	Interrupción de producción por pérdida de datos críticos.

Nota: Riesgos cibernéticos identificados en la infraestructura TI asociada a los procesos OT de la cadena de producción del sector flexográfico colombiano en 2025. Para detalle ver Anexo Nro. 4 (.xlsx). Fuente: Autoría propia.

Al efecto, la Tabla 12, elaborada según las guías de [16] y [18] y reconfirmada por [25], presenta el listado general de los riesgos cibernéticos identificados en el sector flexográfico como producto del análisis de los resultados obtenidos en las actividades 1.1 (diagnóstico de ciberseguridad sectorial) y 1.2 (Análisis y evaluación del riesgo informático) de la fase 1, es decir, reúne los riesgos cibernéticos encontrados como producto de la elaboración de la matriz de riesgo informático del sector industrial de la flexografía.

En cuanto a la matriz de riesgo y su mapa de calor, considerados bajo el contexto de la ciberseguridad, como bien apuntan [15] y [16], su aplicación facilita la toma de decisiones estratégicas y la implementación de controles proporcionales a la magnitud de las amenazas, contribuyendo así a desarrollar, o fortalecer, la continuidad y resiliencia de los sistemas informáticos de la infraestructura TI que, gestionan, operan y controlan los procesos productivos y, por tanto, constituyen un fundamento esencial para el desarrollo del diseño del modelo de ciberseguridad aquí propuesto. Para mayores detalles, la matriz de riesgo y su mapa de calor se consignan en completitud y detalle en el Anexo Nro. 4 (archivo excel) adjunto a esta tesis de maestría.

4.2 Resultados de la fase 2 respecto a la revisión de los estándares y referentes internacionales y las buenas prácticas de seguridad informática y consolidación del diseño del modelo de ciberseguridad para la infraestructura TI asociada a la cadena productiva

Una vez finalizadas las dos (2) actividades de la fase 1, diagnóstico y análisis y evaluación del riesgo cibernético, se emprendió el desarrollo de la fase 2, cuyos resultados se muestran a continuación y que, fundamentalmente, consistieron en la selección de controles acorde a la revisión de estándares y referentes internacionales (considerando el análisis y evaluación del riesgo estimado en la fase 1) y en la consolidación del diseño del modelo de ciberseguridad buscado para la infraestructura TI asociada a la cadena productiva del sector.

En general, la fase 2 consistió en realizar una revisión, detallada y profunda, de los principales estándares internacionales y de las buenas prácticas de seguridad informática en aras a seleccionar los controles y contramedidas adecuados. Este análisis de referentes y estándares se puede ver consolidado en la tabla de controles seleccionados que se puede apreciar en el Anexo Nro. 5 de esta tesis. Según [16] y [18], estos controles brindarán una protección eficaz y efectiva al a infraestructura computacional e informática asociada a la gestión de los procesos OT que soportan la cadena y procesos productivos críticos y esenciales de las PYMEs y empresas de la industria flexográfica e incluyó, siguiendo las recomendaciones de [25], la consolidación del modelo de ciberseguridad propuesto, que se presenta en el Anexo Nro. 6 de esta tesis de maestría en seguridad informática.

4.2.1 Resultados de la Actividad 2.1 de la fase 2

La caracterización de los elementos aplicables derivados de los estándares internacionales y de las buenas prácticas de seguridad informática, siguiendo las recomendaciones de [25] y los lineamientos conceptuales del nuevo marco CCCI planteados en [49], fueron realizadas mediante la selección de los controles adecuados en aras de lograr el mayor nivel de mitigación y reducción posibles en el grado de riesgo informático inicialmente diagnóstica, lo cual dio lugar a la consolidación del diseño del modelo de ciberseguridad propuesto en esta tesis de maestría en seguridad informática. Los controles seleccionados y que forman parte integral del modelo de ciberseguridad propuesto para la infraestructura TI, se presentan en detalle, en el Anexo Nro. 5 (archivo excel).

4.2.2 Resultados de la Actividad 2.2 de la fase 2

A continuación, se consignan los resultados de la actividad 2.2 que, básicamente, consistió en la consolidación del prototipo protectivo cibernético para la infraestructura informática asociada a la cadena de producción crítica de la industria flexográfica, a saber:

4.2.1.2.1 Modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción crítica del sector flexográfico

El modelo de ciberseguridad planteado para la infraestructura informática asociada a la cadena de producción crítica de la industria flexográfica está compuesto por doce (12) pasos o etapas que van desarrollando las capacidades cibernéticas protectivas en la organización. Sin embargo, las compañías cuentan con libertad de adopción y adaptación de los pasos del prototipo cibernético protectivo, puesto que, los pasos propuestos no necesariamente tienen que implementarse en estricto orden y las empresas tienen total flexibilidad para ir incorporando cada paso, de manera paulatina y gradual, hasta completarlos todos.

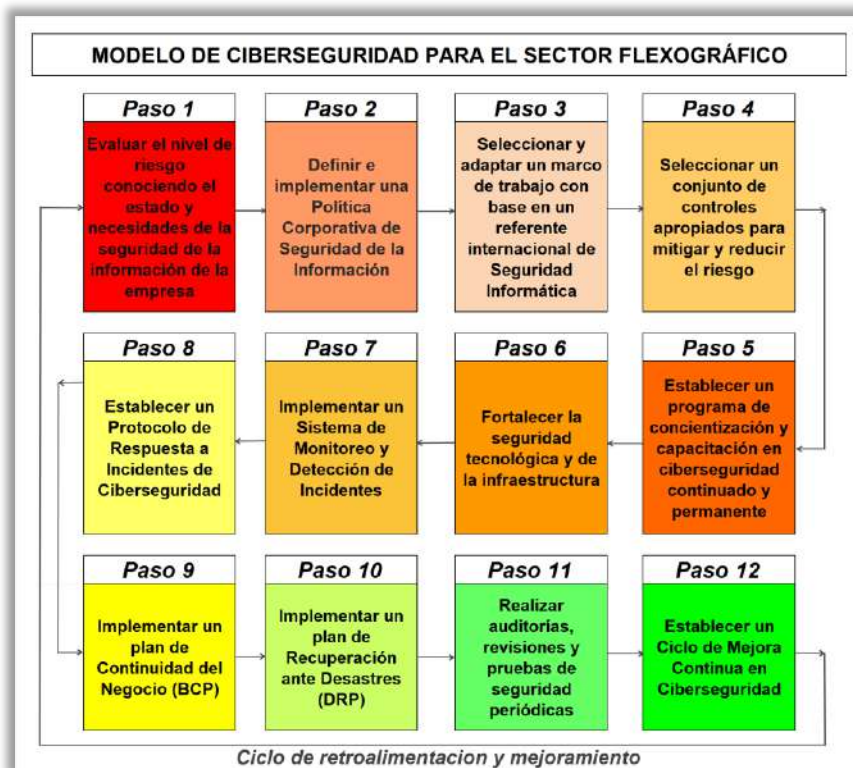


Fig. 13. Modelo de ciberseguridad para la infraestructura informática asociada a la gestión de los procesos OT de la cadena crítica del sector flexográfico.

Nota: Dodecálogo de ciberseguridad (Fase 2, Actividad 2.2. Entregable). Fuente: Autoría propia.

Cada uno de los pasos va fortaleciendo la capacidad defensiva de la organización y creando y fomentando una valiosa cultura de la ciberseguridad en el personal corporativo. La Fig. 13 presenta el modelo de ciberseguridad consolidado que, fundamentalmente, consiste en un dodecálogo compuesto por una metodología paso a paso, donde cada paso va aportando a algún aspecto importante y necesario para lograr la defensa en profundidad de la infraestructura informática asociada a la cadena de producción sectorial.

Como se observa, cada empresa, acorde a sus propias particularidades y circunstancias, deberá llevar a cabo la realización e implementación de cada uno de los pasos propuestos en el prototipo cibernético protectivo, en el orden y temporalidad deseada, para que, al momento de finalizar la adopción y establecimiento de todos los pasos, pueda asegurar la protección y defensa de la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura informática asociada a su cadena de producción.

No obstante, y aun cuando lo más recomendable es comenzar la adopción por el paso 1, el modelo de ciberseguridad otorga la flexibilidad suficiente para que una determinada compañía inicie su implementación por el paso que quiera o que le sea más conveniente o adoptable. Esto es ampliamente beneficioso para el caso de las PYMEs pues sus limitaciones demandan un mecanismo adaptativo y flexible.

Sin embargo, el resultado final de implementación de todos los pasos, finalmente, conducirá a un ciclo de mejoramiento de la ciberprotección y la defensa del sistema informático debido a que el prototipo de ciberseguridad fue fundamentado en el ciclo Deming (ciclo PHVA). El modelo de ciberseguridad así planteado para la infraestructura TI vinculada a la cadena de producción esencial del sector queda, así, inmerso en un permanente lazo cerrado de acciones de mejoramiento.

En este punto, no debe olvidarse que, un aspecto fundamental para asegurar una ciberdefensa en profundidad y, simultáneamente, una tarea necesaria para completar el prototipo cibernético protector para la infraestructura TI, es acometer en un trabajo futuro, el desarrollo de un modelo de ciberseguridad para la adecuada protección y aseguramiento de las tecnologías OT asociadas a la cadena y procesos de producción críticos del sector bajo análisis.

4.2.1.2.2 Pasos y actividades de implementación del modelo de ciberseguridad para la infraestructura IT asociada a la cadena de producción crítica del sector flexográfico

A continuación, se presenta en detalle, la explicación metodológica de cada una de las fases o pasos a implementar para la adopción del modelo de ciberseguridad propuesto para la protección de la infraestructura informática asociada a la cadena de producción crítica del sector flexográfico por parte de una de sus PYMEs o empresas, la cual, como ya se comentó, se compone de doce (12) pasos o etapas. Los apartes siguientes presentan la definición conceptual de cada paso y cada una de las actividades y subactividades que es recomendable desarrollar durante la implementación, a saber:

- **Paso 1.**

Evaluar el nivel de riesgo conociendo el estado y necesidades de la seguridad de la información de la empresa

La evaluación de riesgos es la base de la protección efectiva que brinda el modelo de ciberseguridad, ya que permite identificar vulnerabilidades en la infraestructura digital. Al efecto, y como sugieren [16] y [18], se debe aplicar una metodología formal (ISO 27005, OCTAVE, o NIST, etc.) para calcular probabilidad e impacto de los eventuales ciberincidentes, categorizando activos críticos de la infraestructura informática.

El resultado del análisis y evaluación del riesgo, como puntualiza [25], permite priorizar los recursos en áreas de mayor exposición, lo cual

constituye lo más recomendable como paso inicial en la implementación u adopción de un modelo. Sin embargo, la estructura propuesta permite iniciar el proceso de adopción por el paso que se considere pertinente, pues, al final, el modelo de ciberseguridad es cíclico.

- Realizar un autodiagnóstico preliminar basado en la norma ISO 27001 o en el marco NIST CSF 2.0, o cualquier otro estándar internacional.
- Evaluar el nivel de riesgo informático utilizando una matriz de riesgos alineada con los procesos críticos de la empresa, de manera similar a como se realizó en esta tesis de maestría en seguridad informática.

- **Paso 2.**

Definir e implementar una Política Corporativa de Seguridad de la Información

Una política de seguridad informática es otra base fundamental del modelo de ciberseguridad y se recomienda que, como puntualiza [25], aparte de ser adaptada a las necesidades y requerimientos de la empresa, este alineada con la norma ISO 27001, estableciendo las directrices estratégicas y las obligaciones mínimas que se deben considerar para proteger la información sensible. La relevancia organizacional y la importancia estratégica de contar con una política que guíe y enrute las acciones de ciberseguridad es esencial en cualquier empresa.

- Elaborar una Política Corporativa de Seguridad Informática acorde a las particularidades de la empresa.
- Difundir y aplicar la Política corporativa de seguridad informática, asegurando su comprensión en todos los niveles.

- **Paso 3.**

- Seleccionar y adaptar un marco de trabajo con base en referentes internacionales de seguridad informática**

Como sugieren [16] y [18] y reconfirma [25], adoptar referentes internacionales ampliamente aceptados, combinando o eligiendo entre la familia normativa ISO 27000 series, el marco como NIST CSF 2.0 CSF y los CIS Controls, permitirá lograr la estandarización de los procesos de protección digital y orientar, de manera más precisa y práctica, la gestión de la seguridad informática en una empresa.

Para las PYMEs y demás compañías de la industria flexográfica, lo más recomendable desde la perspectiva de la efectividad, eficacia y la practicidad protectiva es realizar una combinación, optando por una mezcla híbrida de controles seleccionados, como los presentados en el Anexo Nro. 5, ajustando la complejidad técnica con la practicidad y la viabilidad económica de los costos de inversión requeridos; pues, esto asegura una protección digital integral sin sobrecargar el presupuesto organizacional, particularmente, en el caso de las PYMEs, mientras que facilita la adopción del modelo de ciberseguridad y se logran mejores resultados en la protección y defensa cibernética.

- Elegir el marco de referencia internacional preferido: alguno o varios entre:
 - Norma ISO 27001,
 - marco NIST 2.0 CSF
 - CIS Controls, u otro reconocido).
 - Otros que se juzguen o encuentren convenientes.

- Adaptar el referente internacional elegido a la estructura, tamaño y recursos disponibles en la empresa.

- **Paso 4.**

Seleccionar un conjunto de controles apropiados para mitigar y reducir el riesgo

La selección de controles adecuados, pertinentes, efectivos y eficaces, como establecen [16] y [18] y como reconfirma [25], es otra etapa clave de la protección cibernética, la cual, acorde con las particularidades de cada empresa, debe efectuarse considerando la priorización y la proporcionalidad respecto al nivel de riesgo cibernético al elegir adecuadamente cada uno de los controles.

Como orienta [22], de similar manera, la criticidad de los activos informáticos debe ser considerada para que la selección de los controles sea idónea, efectiva y eficaz. Complementariamente, y según sugieren [16] y [18], los controles seleccionados deberán mapearse contra los estándares elegidos para garantizar su consistencia y contar con capacidad de auditoría futura.

- Identificar controles alineados a los riesgos críticos detectados.
- Priorizar la implementación según impacto en la continuidad del negocio y en factibilidad práctica de su aplicación.

- **Paso 5.**

Establecer un programa de concientización y capacitación en ciberseguridad continuado y permanente

El factor humano es el eslabón más débil y uno de los mayores vectores de ciberataque, como puntualiza [26], razón por la que un programa de capacitación y formación continua ayuda a mitigar los riesgos, mejorar la

ciberdefensa y fortalecer la posición de seguridad informática. En particular, en el caso de la industria flexográfica este paso es crucial y obligatorio y quizá el que, en el corto plazo y con mayor inmediatez, ha de brindar unos mejores resultados protectivos.

En efecto, entrenar, tanto a personal directivo, como administrativo, comercial, de mercadeo, de logística, de servicios generales y, también, al personal operativo y de planta que, puede, o no, interactuar con sistemas informáticos y computacionales, garantizará atender esta falencia y mitigar el riesgo informático de las infraestructuras TI, pues este paso garantiza que todos en la organización reconozcan ciberamenazas y apliquen protocolos básicos de seguridad, fomentando la cultura de ciberseguridad.

- Diseñar programas de formación continua que incluya simulacros de ingeniería social, como phishing y buenas prácticas de manejo de la información y uso seguro de los dispositivos.
- Utilizar el nuevo marco CCCI como herramienta pedagógica y didáctica de capacitación. Opcionalmente, se sugiere utilizar el nuevo marco CCCI, que se tratará posteriormente en mayor detalle, permite implementar este paso de manera más sencilla y comprensible para el personal no especializado en ciberseguridad de las empresas.

- **Paso 6.**

Fortalecer la seguridad tecnológica y de la infraestructura

La protección tecnológica requiere de la aplicación de técnicas y procedimientos de hardening para la infraestructura informática, incluyendo hardware, software, aplicativos, redes y bases de datos, como establecen [16] y [18]. De otra parte, incorporar principios de seguridad como Zero Trust Architecture permitirá mejorar automáticamente el nivel de protección de las infraestructuras y activos críticos.

- Implementar medidas técnicas: firewalls, segmentación de red, cifrado, backups, autenticación multifactor (MFA), etc.
- Asegurar la actualización periódica de sistemas y aplicaciones (Parcheo).
- Disponer cualquier otra medida de seguridad técnica que se considere necesaria, en particular, esta misma consideración debe tenerse muy en cuenta y ejecutarse, para completar este modelo protector TI, realizando la adecuada protección de la propia infraestructura OT.

- **Paso 7.**

- **Implementar un sistema de monitoreo y detección de incidentes**

Según sugiere [27], el monitoreo continuo de la infraestructura y activos informáticos críticos, adoptando un SIEM como Azure Sentinel, de pago, o, Wazuh, open source, permitirá a las PYMEs y empresas, correlacionar eventos cibernéticos y detectar anomalías en tiempo real. En la industria flexográfica, es clave vigilar el tráfico de red, los accesos no autorizados, los intentos de intrusión, entre otros, pues, esto reduce significativamente la ventana de exposición ante ciberataques.

- Desplegar herramientas de monitoreo (SIEM, IDS/IPS, EDR) siendo posible optar por alternativas de pago u open source según la capacidad particular de la compañía.
- Establecer métricas de detección temprana y alertas sobre anomalías en la red y sistemas.

- **Paso 8.**

- **Establecer un protocolo de respuesta a incidentes de ciberseguridad**

Un plan de respuesta formal que defina roles, responsabilidades y flujos de comunicación ante ciberincidentes, que incluya procedimientos de contención, aislamiento, análisis forense digital, erradicación y recuperación, contribuye sustancialmente a mitigar el riesgo informático, según apunta [16], pues, en un entorno productivo como el industrial, la rapidez de respuesta es esencial para evitar la detención de la cadena de producción, en particular, de las líneas de impresión flexográfica, redundando en mayor capacidad de continuidad y resiliencia operacional.

- Diseñar un plan de manejo de incidentes de seguridad, con roles y responsabilidades claramente definidos y asignados.
 - Formar un CSIRT interno (o externo) para la gestión y documentación de incidentes cibernéticos extrayendo las lecciones aprendidas.

- **Paso 9.**

- **Implementar un plan de continuidad del negocio (BCP)**

El BCP ayuda a robustecer la operatividad mínima de los procesos críticos aún bajo ciberataque o fallo tecnológico, en razón a que contempla alternativas procedimentales claras y predefinidas para mantener, o restablecer con inmediatez, la operación de la cadena de producción, aunque los sistemas informáticos estén comprometidos, según destaca la contribución investigativa de [12]. En la industria flexográfica esto puede significar la priorización manual de órdenes y mantener sistemas de respaldo para fortalecer la continuidad y la resiliencia operacionales, practicando la premisa estratégica de prepararse para lo peor, mientras se espera lo mejor, como sugiere [27].

En este contexto, es importante el establecimiento de un ciclo de mejora continua y actualización del BCP, asegurando que los procedimientos evolucionen conforme a los cambios en la infraestructura tecnológica, los nuevos riesgos emergentes (como ciberataques) y los resultados obtenidos en las pruebas periódicas, fomentando, además, la cultura de resiliencia en la organización. Es de tomar en cuenta que, para completar este modelo de ciberseguridad, como actividad futura, se deberá incluir la protección de la infraestructura OT.

- Adaptar e implementar un plan de Continuidad (BCP), de tal manera que queden definidas las estrategias de pronto restablecimiento digital y las actividades mínimas necesarias para mantener las operaciones críticas.
- Realizar pruebas periódicas de continuidad.

- **Paso 10.**

- Implementar un plan de recuperación ante desastres (DRP)**

El DRP, como destacan [12], establece procedimientos para restaurar la infraestructura tecnológica tras un ciberincidentes mayor (malware, ransomware, fallos de servidores, calamidades o desastres, etc.), razón por la que incluye alternativas de protección como copias de seguridad, redundancia en la nube, planes de restauración de sistemas y de software, con tiempos de recuperación (RTO/RPO) definidos según criticidad.

- Adaptar e implementar un plan de Recuperación de Desastres (DRP), de tal manera que queden definidas las estrategias de resiliencia digital mínimas necesarias para resistir eventos imprevistos y súbitos manteniendo las operaciones críticas.
- Realizar pruebas periódicas de recuperación.

- **Paso 11.**

- **Realizar auditorías, revisiones y pruebas de seguridad periódicas**

Las auditorías de seguridad informática, como plantea [26], permiten verificar el cumplimiento de los controles y detectar las brechas de ciberseguridad. Se recomienda combinar revisiones de cumplimiento acordes con la norma ISO 27001 con pruebas de naturaleza técnica, como procedimientos de pentesting, escaneo de vulnerabilidades, et al. Para la industria flexográfica, estas revisiones y evaluaciones deben cubrir tanto los entornos informáticos de la cadena de producción interconectados al ciberespacio o a otras redes, como también, las demás redes de la empresa.

- Efectuar auditorías internas (y, eventualmente, externas).
 - Realizar pruebas de penetración (pentesting), vulnerabilidad y análisis forense preventivo acorde con la capacidad de la compañía.

- **Paso 12.**

- **Establecer un ciclo de mejora continua en ciberseguridad**

El ciclo Deming o ciclo PHVA, como apuntan [12], es otra de las bases fundamentales del modelo de ciberseguridad propuesto, pues, asegura que el sistema de seguridad informática evolucione frente a nuevas ciberamenazas, mejorando continuamente y aprovechando el poder de la retroalimentación. Involucra actualizar políticas, ajustar controles, reevaluar riesgos e implementar las lecciones aprendidas tras auditorías o análisis forenses digitales (en caso de ciberincidentes), pues permite que la empresa mantenga y fortalezca su capacidad de continuidad y resiliencia digital en el tiempo. Al respecto, debe hacerse notar que, el ciclo de Deming o ciclo PHVA es el motor que transforma la ciberseguridad desde un esfuerzo reactivo y aislado para convertirlo en un sistema de gestión resiliente, proactivo y dinámico.

- Aplicar el ciclo Deming (Ciclo PHVA con Planear, Hacer, Verificar y Actuar) como parte de la estrategia de ciberseguridad corporativa.
- Retroalimentar el modelo con lecciones aprendidas de incidentes, auditorías y cambios regulatorios, de negocios, de tecnologías, etc.
- Estructurar la documentación de los procedimientos de seguridad informática.
- Definir indicadores de gestión para medir la eficacia del modelo de ciberseguridad implementado.

En general, se puede observar que el modelo de ciberseguridad propuesto destaca por su enfoque integral, diseñado no solo para proteger activos informáticos, sino para desarrollar la resiliencia operativa ante cualquier evento disruptivo. En efecto, una de sus principales bondades es que no se limita a la implementación tecnológica; por el contrario, construye una base sólida desde la gestión estratégica con la evaluación de riesgos y la definición de políticas corporativas claras. De otra parte, al integrar pasos específicos para la concienciación, sensibilización, capacitación y entrenamiento del personal en ciberseguridad y establecer la creación de protocolos de respuesta, el prototipo cibernético protectivo desarrollado reconoce que la protección de la triada de la CIA de la seguridad de la información depende tanto de las herramientas digitales como de la cultura organizacional y la capacidad de reacción humana.

Otra ventaja competitiva del esquema propuesto es su énfasis en dos aspectos neurálgicos como son la continuidad y la resiliencia, aunados a la mejora y al fortalecimiento constante a través de la retroalimentación que se logra con el aporte del ciclo de Deming. En este sentido, a diferencia de los modelos tradicionales, que suelen ser estáticos, el prototipo cibernético protectivo propuesto incluye capas explícitas de recuperación (BCP y DRP) que definen estrategias de restablecimiento digital para mantener las operaciones críticas

incluso en casos de crisis. Finalmente, la inclusión de revisiones, auditorías, simulacros, pruebas de pentesting y el uso de un ciclo de retroalimentación aseguran que sea adaptable y escalable, permitiendo a las empresas evolucionar sus defensas frente a nuevas ciberamenazas y cambios tecnológicos, garantizando así una protección eficiente a largo plazo.

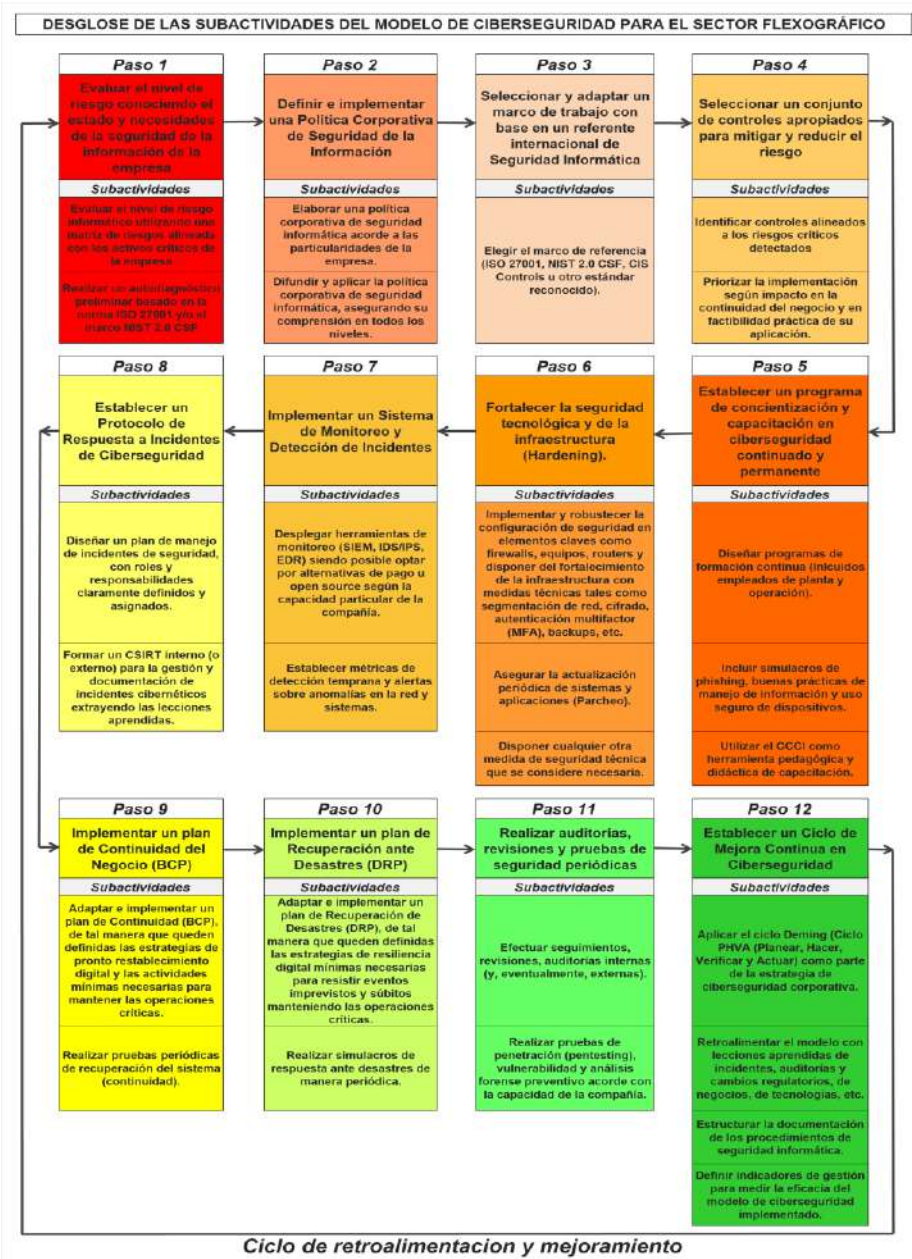


Fig. 14. Modelo de ciberseguridad para la infraestructura TI asociada a la gestión de la cadena de producción crítica de la industria flexográfica. Desglose completo con actividades.
Nota: Desglose bidimensional con actividades y subactividades (Fase 2, actividad. 2.2). Ver Anexo Nro. 6 en mayor detalle y completitud. Fuente: Autoría propia.

En la Fig. 14 se muestran, en forma esquemática, las actividades asociadas a la implementación del prototipo cibernético protectivo desarrollado. El procedimiento diseñado describe un enfoque integral y cíclico que, inicia con el paso de la identificación y evaluación de riesgos, seguida de la definición de políticas corporativas y la adopción de marcos internacionales reconocidos para seleccionar y priorizar controles alineados con los riesgos críticos y la continuidad del negocio y así seguidamente.

Como se aprecia, cada paso conlleva la ejecución de las actividades y subactividades propuestas. No obstante, y como se puntualizó anteriormente, las compañías tienen libertad de elección de con cual paso iniciar, o sobre qué pasos pueden ir adoptando, pues, no se trata de una camisa de fuerza, sino, más bien de una orientación hacia la defensa en profundidad, bajo la consigna importante de realizar, con el tiempo, la implementación de todos los pasos del prototipo cibernético protectivo a fin de asegurar la protección de la triada de la CIA de sus sistemas informáticos.

De manera complementaria, como puede apreciarse de la Fig. 14, el modelo cibernético protectivo propuesto para los sistemas TI de gestión y que soportan el proceso OT de la cadena de producción de la industria flexográfica, también incorpora, de manera integral y equilibrada, la impronta de los lineamientos derivados del nuevo marco CCCI propuestos por [23], [24] y [49], el cual que puede observarse en detalle el Anexo Nro. 11 de esta tesis.

Allí se incluyen las dimensiones originales de McCumber (triada CIA: confidencialidad, integridad y disponibilidad de la información, estados de la información y aspectos procedimentales, humanos y tecnológicos) y se incorporan la dimensión de los estándares internacionales, la implementación operativa y la continuidad y resiliencia, para lo cual se apoya en programas permanentes de concientización y capacitación, el fortalecimiento de la infraestructura mediante medidas de hardening, monitoreo y detección de incidentes, así como en protocolos formales de respuesta y gestión de ciberincidentes.

Complementariamente, y como sugieren [12], el prototipo cibernético protectivo propuesto también, contempla con especial atención la implementación de planes de continuidad del negocio y recuperación ante desastres, respaldados por pruebas periódicas, revisiones, auditorías y evaluaciones técnicas, consolidándose, finalmente, como un ciclo de mejora continua que permite adaptar y optimizar la estrategia de ciberseguridad frente a cambios operativos, tecnológicos y regulatorios, garantizando su efectividad y sostenibilidad en el tiempo.

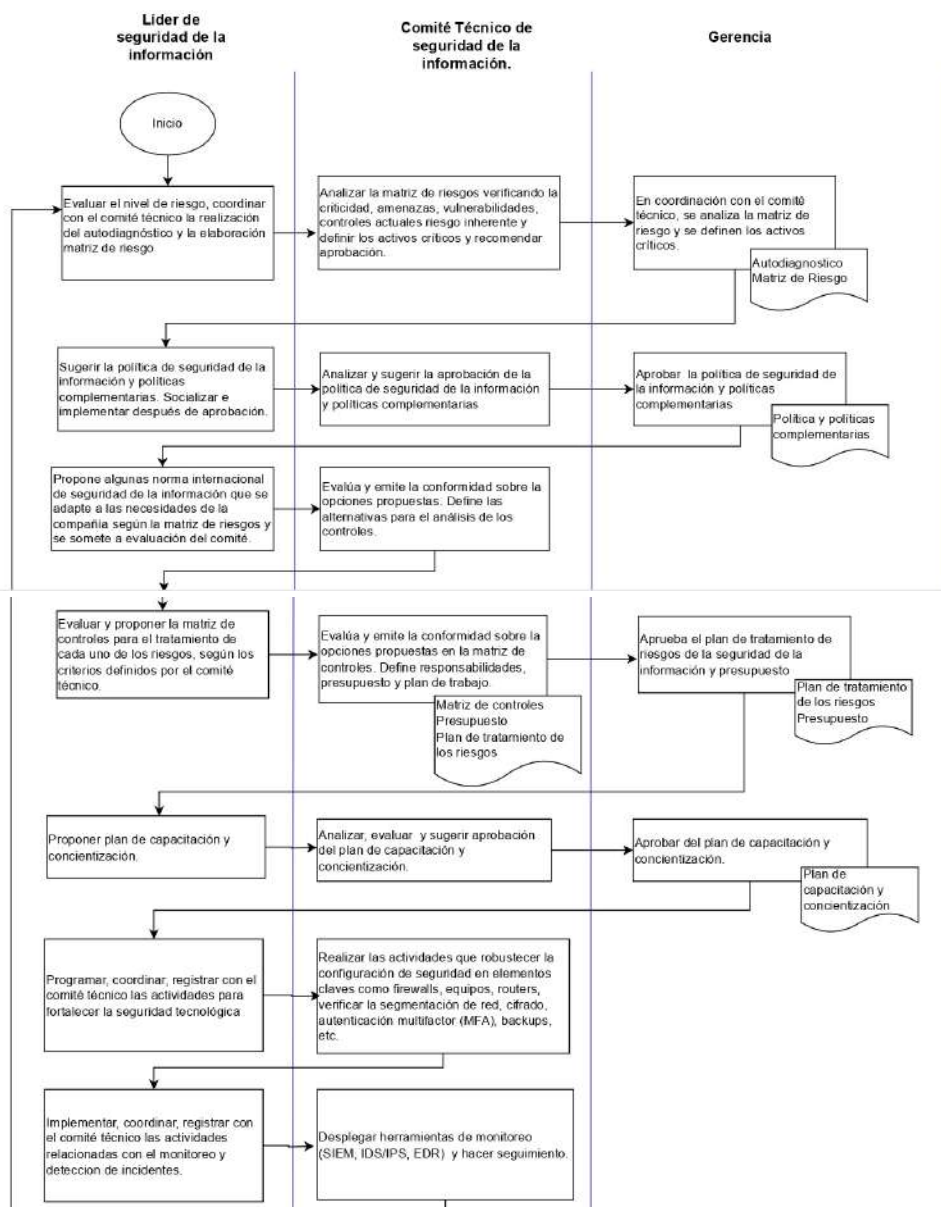
En este punto es menester resaltar que, según plantean [15], [16], [18] y reconfirma [25], aunado a las recomendaciones derivadas de los estándares internacionales y las buenas prácticas de ciberseguridad, una implementación lógica del modelo cibernético protectivo propuesto debería, o por lo menos, es aconsejable que sea iniciada en su adopción, con el análisis y evaluación del riesgo (paso 1), tal como presentan [49] y aun cuando, para la realidad de las PYMEs de las diversas industrias esenciales, solo se trata de una sugerencia de naturaleza técnica dentro de la lógica de la seguridad informática.

4.2.1.2.3 Diagrama de flujo para adopción práctica del modelo de ciberseguridad propuesto

La implementación de un prototipo cibernético protectivo como el desarrollado se facilita mucho con un diagrama de flujo, el cual muestra, de manera didáctica y sencilla, una visualización, a modo de ejemplo, de la forma práctica mediante la cual una compañía, acorde con su realidad empresarial, puede realizar la adopción del modelo de ciberseguridad propuesto en su infraestructura TI asociada a su cadena de producción, solo siguiendo un derrotero sencillo de actividades, como el presentado en el camino que muestra el flujograma, de tal manera que le permita ir mejorando la protección de sus sistemas informáticos paulatina, gradual, pero, firmemente.

Como se aprecia a continuación, en la Fig. 15, se presenta el diagrama de flujo recomendado para la adopción e implementación del modelo de ciberseguridad

propuesto en una empresa dada, pues, se trata de una herramienta gráfica y visual muy útil para orientar la adopción y adaptación del diseño del prototipo cibernético protectivo desarrollado, tanto en el caso de las PYMEs, como de otras empresas del sector flexográfico, pues, su potencialidad permite representar, de manera clara, práctica y sencilla, cada uno de los pasos, etapas, actividades primarias y secundarias (subactividades) requeridas para la implementación exitosa del modelo de ciberseguridad desarrollado por parte de una determinada compañía que decida optar por su implementación.



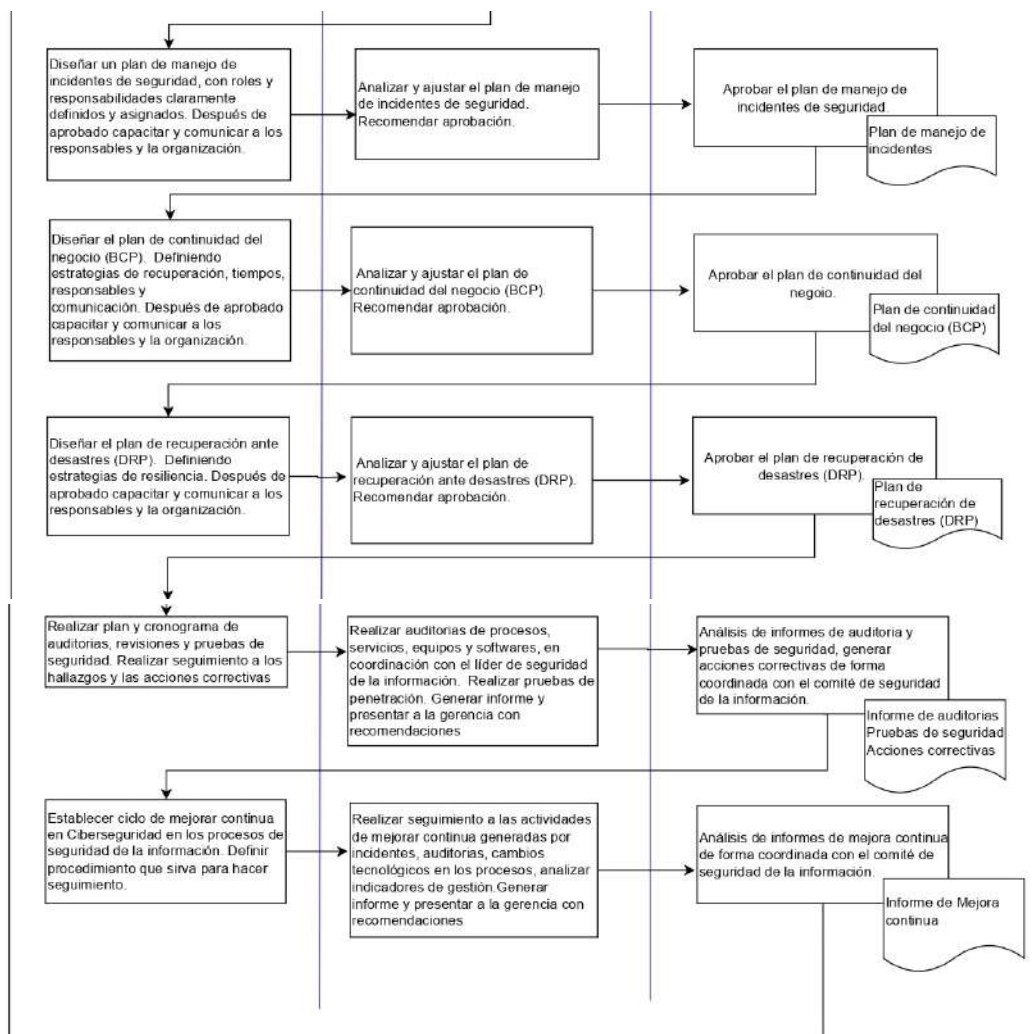


Fig. 15 Diagrama de flujo para aplicación práctica del modelo de ciberseguridad.

Nota: Desglose de pasos para aplicación práctica del modelo de ciberseguridad. Fuente: Autoría propia.

Las actividades, procesos, decisiones y controles del diagrama de flujo, presentados en la Fig. 15, e involucrados en la labor de protección de la seguridad de la información de la infraestructura TI asociada a la cadena de producción, permiten realizar el mapeo del flujo de datos, los puntos de entrada, las rutas de procesamiento, la identificación de vulnerabilidades y ciberamenazas, los posibles riesgos, las brechas de seguridad, definir políticas, seleccionar tecnologías de protección, establecer planes de contingencia, verificar redundancias en los controles y, muy importante, también, permite validar el diseño del propio modelo de protección digital personalizado que haya sido adoptado por una compañía específica.

Es de resaltar, nuevamente, que el diagrama de flujo presentado en la Fig. 15, tiene la versatilidad y flexibilidad para poder ser asumido (al igual que el propio modelo de ciberseguridad propuesto) por parte de una empresa o PYME, desde cualquiera de las fases o pasos sugeridos (no necesariamente se tiene que iniciar por el paso 1), en razón a que el prototipo protectivo cibernético, en sí mismo, es un ciclo continuo y de permanente retroalimentación y mejoramiento, pues, está basado en el ciclo Deming, o ciclo PHVA, propio de los estándares internacionales promovidos por la ISO.

4.2.1.2.4 Análisis de la mitigación de riesgos con el modelo de ciberseguridad propuesto.

Al respecto, es importante considerar el análisis de la mitigación de riesgos que, eventualmente, pueden lograr las empresas con la adopción del modelo de ciberseguridad propuesto y vale resaltar que el prototipo cibernético protectivo desarrollado para el sector flexográfico funciona como un escudo estratégico que reduce, de manera progresiva, paulatina y gradual, los riesgos informáticos críticos que amenazan la estabilidad de la infraestructura computacional e informática que opera, gestiona y controla la cadena de producción crítica de las PYMEs y empresas de la industria flexográfica.

Como ejemplo, obsérvese que, el prototipo protectivo digital propuesto contribuye significativamente a la mitigación del riesgo de interrupción operativa; pues, mediante la implementación de planes de continuidad y recuperación de desastres, las empresas minimizan la posibilidad de que un ataque de *ransomware*, un malware o un fallo técnico, detenga o colapse la infraestructura informática de la cadena productiva por tiempo prolongado, lo que previene pérdidas financieras masivas y el incumplimiento de plazos de entrega para con los clientes. Para mayor claridad, a continuación, la Tabla 12 presenta un resumen de como cada paso del prototipo protectivo digital desarrollado contribuye a la mitigación de los riesgos cibernéticos encontrados en el sector flexográfico.

Tabla 13. Resumen del análisis de la mitigación de riesgos cibernéticos identificados en la infraestructura TI asociada a la cadena de producción de la industria flexográfica con el modelo de ciberseguridad propuesto.

Paso del Modelo de Ciberseguridad	Riesgos que mitiga	Explicación de la mitigación	Riesgo	Descripción del Riesgo
Paso 1: Evaluar el nivel de riesgo conociendo el estado y necesidades de la seguridad...	R9, R10	Al realizar un autodiagnóstico basado en NIST 2.0 CSF, se identifica la exposición de red y configuraciones incorrectas antes de que sean explotadas.	R1	Infección de equipos, cifrado de datos y pérdida de productividad.
Paso 2: Definir e implementar una Política Corporativa de Seguridad de la Información.	R11	Ataca directamente la pérdida de control interno y fuga de información mediante reglas claras para todos los niveles.	R2	Secuestro o corrupción de datos críticos y manipulación.
Paso 3: Seleccionar y adaptar un marco de trabajo con base en un referente internacional...	R3, R11	Mitiga el robo de datos y pérdida de control al usar estándares como ISO 27001, que obligan a proteger activos críticos.	R3	Robo de datos confidenciales y pérdida de respaldo físico.
Paso 4: Seleccionar un conjunto de controles apropiados para mitigar y reducir el riesgo.	R12	Permite priorizar la protección de "formulaciones y condiciones de máquina" al identificar controles alineados a riesgos críticos.	R4	Caída de la red, interrupción del negocio y malware.
Paso 5: Establecer un programa de concientización y capacitación en ciberseguridad...	R8	Es la defensa principal contra el "Error humano, mal uso del sistema, alteración o manipulación".	R5	Fallos por falta de soporte y explotación de malware.
Paso 6: Fortalecer la seguridad tecnológica y de la infraestructura (Hardening).	R1, R4, R5, R6	Al usar firewalls, MFA y parches, evita la infección de equipos, caídas de red y fallos por falta de soporte.	R6	Ataques dirigidos, robo de credenciales, malware y ransomware.
Paso 7: Implementar un Sistema de Monitoreo y Detección de Incidentes.	R6, R7, R9	Detecta ataques dirigidos, escalada de privilegios y fugas de información mediante herramientas como SIEM o EDR.	R7	Escalada de privilegios y ataques del día cero.
Paso 8: Establecer un Protocolo de Respuesta a Incidentes de Ciberseguridad.	R2, R13	Reduce el impacto del secuestro de datos al tener un equipo (CSIRT) que sabe cómo actuar ante la crisis.	R8	Error humano, mal uso del sistema o manipulación.
Paso 9: Implementar un plan de Continuidad del Negocio (BCP).	R4, R13	Mitiga la interrupción del negocio asegurando que existan estrategias para el pronto restablecimiento digital.	R9	Exposición de red o sistemas internos y fuga de información.
Paso 10: Implementar un plan de Recuperación ante Desastres (DRP).	R1, R2, R13	Ataca el cifrado de datos y pérdida de productividad mediante simulacros y restauración de sistemas.	R10	Sabotaje, configuraciones incorrectas o exposición de datos.
Paso 11: Realizar auditorías, revisiones y pruebas de seguridad periódicas.	R5, R7, R10	Identifica ataques de día cero y configuraciones incorrectas mediante pentesting y auditorías externas.	R11	Pérdida de control interno y fuga de información.
Paso 12: Establecer un Ciclo de Mejora Continua en Ciberseguridad.	Todos (R1-R13)	Evita que el modelo quede obsoleto, retroalimentándolo con lecciones aprendidas de incidentes reales.	R12	Pérdida de fórmulas, condiciones de máquina y especificaciones.
			R13	Interrupción de producción por pérdida de datos críticos.

Nota: Resumen del análisis de la mitigación de riesgos identificados en la infraestructura TI asociada a la cadena de producción de la industria flexográfica con el modelo de ciberseguridad propuesto. Para mayor detalle, ver Anexo Nro. 8 de esta tesis de maestría. Fuente: Autoría propia.

En el ámbito técnico, el modelo de ciberseguridad propuesto reduce en gran medida los riesgos informáticos para los sistemas TI, desde intrusiones indeseadas hasta ciberespionaje industrial, pues, al fortalecer la defensa de la infraestructura computacional y aplicar auditorías periódicas, se van cerrando

las brechas que facilitan o permiten el acceso no autorizado a las redes corporativas, en particular, las vinculadas con la gestión, operación y control de la cadena crítica de producción sectorial.

Esto se complementa con una reducción significativa de la superficie de exposición derivada de la mitigación del nivel del riesgo y su probabilidad de ocurrencia por causa, en especial, del factor humano, ya que el prototipo cibernético protectivo propuesto incluye la adopción e implementación de programas y actividades de capacitación y entrenamiento continuo en ciberseguridad. Así pues, se prepara al personal no especializado, o no experto, en seguridad informática para poder identificar tentativas de ciberataque, en particular, aquellos derivados de ingeniería social (phishing, vishing, smishing o farming) que son una de las puertas de entrada más común para las ciberamenazas actuales.

Finalmente, la adopción del modelo cibernético protectivo ayuda sustancialmente a la disminución de los riesgos legales y reputacionales, pues, al alinear la operación de la cadena de producción crítica con estándares internacionales y procesos de mejora continua, las organizaciones evitan sanciones por incumplimiento de normativas de protección de datos y protegen su prestigio ante clientes corporativos de alto nivel que exigen proveedores confiables. Todo mientras brindan una mejor ciberprotección a su infraestructura informática y computacional.

Así pues, el modelo de ciberseguridad desarrollado para la infraestructura TI, termina por transformar una infraestructura computacional vulnerable en un entorno digital más resiliente y seguro, capaz de detectar anomalías a tiempo y reaccionar con orden y organización frente a cualquier ciberincidente, asegurando la continuidad del sistema TI asociado a la de la cadena de producción crítica y conservando la confidencialidad, integridad y disponibilidad de sus sistemas informáticos y, por tanto, velando por la supervivencia del negocio a largo plazo.

4.3 Resultados de la fase 3 respecto a la verificación y validación del modelo de ciberseguridad para los sistemas TI asociados a la cadena de producción de la industria flexográfica

Siguiendo las recomendaciones metodológicas de [57], la fase 3 consistió en la verificación y validación del prototipo cibernético protectivo desarrollado en las fases 1 y 2. Al efecto, se determinó realizar una prueba conceptual a ejecutar mediante un instrumento metodológico aplicado (encuesta de verificación). Luego, como resultado de la fase 3 se logró la validación completa del modelo de ciberseguridad propuesto para los sistemas TI, asegurando la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura informática asociada a la gestión de la cadena de producción crítica de la industria flexográfica.

Como se describió en profundidad en el capítulo 3 de metodología, en esta fase, se desarrolló el método de verificación por medio de la elección de una prueba conceptual, la cual se realizó, acorde a los preceptos de [58], por medio de la aplicación de un instrumento (encuesta de validación del modelo de ciberseguridad aplicada a los mismos clientes que fueron entrevistados en la fase 1) de manera tal que se posibilitó la realización de una estimación comparativa de la mitigación y reducción del riesgo cibernético lograda con el modelo de ciberseguridad propuesto.

4.3.1 Resultados de las actividades de la fase 3

Esta última etapa, como consignan [23], [24] y [49], estuvo conformada, fundamentalmente, por tres (3) actividades, a saber: La actividad 3.1 de determinación y selección de una metodología de validación apropiada; la actividad 3.2 de aplicación de la prueba de validación del prototipo cibernético protectivo y la actividad 3.3 de tabulación y análisis de los resultados obtenidos en la actividad 3.2. A continuación se presentan los resultados obtenidos en cada una de las actividades de esta fase final de investigación, a saber:

4.3.1.1 Aspectos metodológicos del instrumento aplicado

Fundamentalmente, se aplicó una encuesta de verificación, la cual se encuentra disponible en el Anexo Nro. 7, la cual fue aplicada con similares parámetros a la realizada en la fase 1, pero, circunscribiendo su ejecución exclusivamente a las mismas empresas y compañías inicialmente encuestadas a fin de lograr un marco comparativo que permitiese conocer el nivel de mitigación o reducción del riesgo logrado con el modelo de ciberseguridad desarrollado para la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica. Por brevedad, se omitirán los detalles propiamente estadísticos, pero, están disponibles en el Anexo Nro. 7 para su consulta o mayor detalle.

4.3.1.2 Resultados de la Actividad 3.1

En este contexto, la actividad 3.1 cuya finalidad fue determinar y seleccionar una metodología de validación apropiada que, al efecto y por conveniencia de método, se decidió por la realización de una prueba conceptual, realizada mediante la aplicación de un instrumento metodológico, para el caso una encuesta de verificación, acorde y según las recomendaciones de [58].

Dicha encuesta fue intitulada “*Validación del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico*” y se muestra, en completo detalle, en el Anexo Nro. 7 de esta tesis. Al efecto, un resumen de las preguntas realizadas en la encuesta final de verificación aplicada para la validación del modelo de ciberseguridad desarrollado para la infraestructura TI analizada, se presenta, a continuación, en la Tabla 14.

Tabla 14. Resumen de la encuesta de validación realizada para la verificación del modelo de ciberseguridad desarrollado para la industria flexográfica.

PREGUNTA NRO.	CUESTIONAMIENTO / PREGUNTA
1	¿En qué nivel cree Ud. que el modelo contribuye a construir o mejorar sus estrategias o planes de seguridad informática y, en general, a mejorar la ciberseguridad?
2	Considerando, en particular, las recomendaciones sobre cómo implementar medidas y controles de seguridad ¿En qué nivel cree Ud. que su adopción contribuiría a la disminución del nivel de riesgo informático ?
3	¿En qué nivel consideraría Ud. que, reforzar su personal de ciberseguridad, ayudaría a mitigar y reducir su nivel de riesgo ante ciberataques e incidentes informáticos?
4	¿En qué nivel implementaría Ud. los pasos que se recomiendan y que se sugieren, entre ellos mejorar los controles de acceso con contraseñas más seguras y el uso de doble factor de autenticación , incluyendo implementar los controles respectivos sugeridos, para mejorar la protección y disminuir el riesgo cibernético?
5	¿En qué nivel consideraría Ud. implementar programas permanentes y continuos de capacitación y actualización en ciberseguridad para todo su personal?
6	¿En qué nivel cree Ud. que fortalecer su sistema de respaldo y recuperación de información de producción (production backup), incluida copia en la nube, sería conveniente, para garantizar la continuidad operativa y la resiliencia de su cadena de producción crítica ?
7	¿En qué nivel considera Ud. que, implementar, de manera periódica, el análisis y evaluación del riesgo informático, con el fin de mitigar riesgos, sería una práctica de seguridad conveniente y recomendable para su empresa?
8	¿En qué nivel considera Ud. que su adopción contribuiría a conseguir, o fomentar, el compromiso de la gerencia con la ciberseguridad y a crear, o fortalecer, una cultura de seguridad informática al interior de su organización?
9	¿En qué nivel considera Ud. que los controles y medidas sugeridos son apropiados para la protección sus redes internas/externas y el aseguramiento de su conexión a internet?
10	¿En qué nivel considera Ud. que su adopción e implementación, contribuiría a la reducción o disminución de impactos negativos ocasionados por ciberataques ?
11	¿En qué nivel considera Ud. que su adopción e implementación, contribuiría al mejoramiento de la gestión de atención y respuesta de incidentes informáticos ?
12	En general, ¿En qué nivel considera Ud. que el modelo de ciberseguridad propuesto protegerá la confidencialidad, integridad y disponibilidad de la seguridad de la información de su cadena de producción crítica?

Nota: Resumen de las preguntas de la encuesta final de validación del modelo de ciberseguridad para los sistemas informáticos asociados a la gestión de la cadena de producción crítica realizada en la industria flexográfica.

Fuente: Autoría propia.

Es importante resaltar que, la encuesta fue dirigida y aplicada a la misma muestra estadística inicial, con miras, no solo a verificar y validar el modelo de ciberseguridad propuesto en esta tesis de maestría, sino, también, por conveniencia metodológica, a fin de poder realizar la estimación del grado de reducción y mitigación del riesgo cibernético inicial logrados, una vez

considerado del modelo de ciberseguridad propuesto, por parte de las empresas del sector flexográfico. En este punto, también, se debe resaltar que, nuevamente, se informó a las empresas encuestadas, al igual que se había hecho durante la fase 1 de diagnóstico sectorial, que el alcance del modelo protectivo digital propuesto incluye exclusivamente los sistemas TI, sin incluir las infraestructuras OT, cuya protección se dejó para un trabajo futuro.

De otra parte, se debe hacer notar que, la configuración elegida de las preguntas confeccionadas en la encuesta final de validación aplicada fue direccionadas a la estimación de la reducción del nivel de riesgo cibernético obtenido mediante la comparación del estado inicialmente diagnosticado de ciberseguridad sectorial y el estado final una vez considerado el prototipo cibernético protectivo propuesto en esta tesis de maestría.

Al efecto, la Tabla 15 presenta la escala de Likert utilizada en la encuesta de validación final:

Tabla 15. Escala de Likert para la encuesta de verificación del prototipo cibernético protectivo desarrollado para la infraestructura TI asociada a la gestión de la cadena de producción de la industria flexográfica.

CONVENCIONES				
ESCALA DE LIKERT PARA VALORACIÓN DE RESPUESTAS DE LA ENCUESTA				
Escala de Valores		Opciones posibles de respuesta		
Letras	Números			
Cero	0	No tiene implementación de Ciberseguridad alguna.	Ninguna	Totalmente en desacuerdo
Uno	1	Tiene solamente una implementación de Ciberseguridad incipiente	Poca	En desacuerdo
Dos	2	Tiene una algún tipo de implementación muy básica de Ciberseguridad que no logra brindar protección completa	Regular	Neutral
Tres	3	Tiene una algún tipo de implementación funcional de Ciberseguridad que brinda un muy moderado nivel de seguridad.	Mucha	De acuerdo
Cuatro	4	Tiene una implementación de Ciberseguridad buena y suficiente.	Casi toda	Muy de acuerdo
Cinco	5	Tiene una implementación de Ciberseguridad completa y total basada en normas y estándares internacionales	Toda	Totalmente de acuerdo

Nota: Se utilizó una escala apropiada para los propósitos de validación del modelo de ciberseguridad propuesto y estimación comparativa de la reducción del riesgo cibernético logrado. Fuente: Autoría propia.

4.3.1.3 Resultados de la Actividad 3.2

Una vez definido el tipo de prueba conceptual a realizar y, según las recomendaciones de [58], se efectuó la aplicación del instrumento metodológico elegido y configurado anteriormente en la actividad 3.1 y cuyos resultados se presentan en el Anexo Nro. 8 de esta tesis de maestría en seguridad informática.

4.3.1.4 Resultados de la Actividad 3.3

A continuación, en la Tabla 16 se consignan un resumen de los resultados obtenidos a las preguntas realizadas con el instrumento aplicado que, como se denota claramente, se concentraron en las valoraciones más altas (4 y 5 en la escala de Likert y ninguna respuesta en menos de 4), lo cual refleja la amplia validación obtenida por el modelo de ciberseguridad desarrollado para los sistemas TI, entre las PYMEs y empresas de la industria flexográfica.

Tabla 16. Resultados de la validación del modelo de ciberseguridad desarrollado.

PREGUNTA NRO.	OPCIÓN DE RESPUESTA (Escala de Likert)					
	0	1	2	3	4	5
1					10	14
2					11	13
3					16	8
4					14	10
5					10	14
6					11	13
7					15	9
8					15	9
9					14	10
10					9	15
11					9	15
12					7	15

Nota: Como se observa, el modelo protectivo para la infraestructura TI vinculada a la gestión de los procesos OT de la cadena de producción crítica de la industria flexográfica fue recibido con amplia favorabilidad y los resultados de su verificación fueron muy buenos entre empresas del sector, particularmente, las PYMEs.

Fuente: Autoría propia.

Esta actividad 3.3 que, siguiendo las guías de [18] y [25], consistió en la tabulación y análisis de los resultados derivados de la aplicación del instrumento metodológico (encuesta final de verificación) definido en la actividad 3.1 y ejecutado en la actividad 3.2, se realizó mediante un procedimiento estadístico y gráfico en excel y análisis su correspondiente análisis de resultados (similar al efectuado con el diagnóstico inicial del estado y requerimientos de ciberseguridad del sector flexográfico (fase 1, actividad 1.1) y es presentado, en detalle, el Anexo Nro. 8 de esta tesis de maestría.

En este punto, es importante hacer notar, que los resultados obtenidos fueron muy buenos, razón por la cual, el prototipo cibernético protectivo desarrollado para la infraestructura TI asociado a la cadena de producción de la industria flexográfica, no tuvo la necesidad de recibir ajuste, ni refinación alguna y que, no se requirió de su pulimentación, pues su efectividad y eficacia en la protección y el aseguramiento de la confidencialidad, la integridad y la disponibilidad de la seguridad de la información de los sistemas e infraestructura informática asociada a la gestión, operación y control de la cadena de producción esencial de la industria flexográfica y a la defensa de la seguridad de la información de PYMEs y empresas del sector bajo estudio, fue satisfactoria y acorde con lo esperado.

Como se observa de la Fig. 16, que complementariamente, presenta el detalle del análisis de Pareto derivado de los resultados obtenidos en la aplicación de instrumento metodológico de validación del prototipo de ciberseguridad y en la cual se evidencia una evolución positiva y altamente significativa en la percepción de utilidad y pertinencia y, también, respecto a la adopción de las recomendaciones y buenas prácticas de ciberseguridad generadas por la consideración del modelo cibernético protectivo propuesto en esta tesis de maestría en seguridad informática. Si bien es cierto que se debe incluir la protección de la infraestructura OT para completar el modelo de ciberseguridad propuesto, como se observa de los hallazgos obtenidos, los problemas de ciberseguridad inicial observados en los sistemas TI presentan una mejora significativa, lo cual repercute en una reducción del nivel de exposición de la superficie de ataque para beneficio de la industria flexográfica.

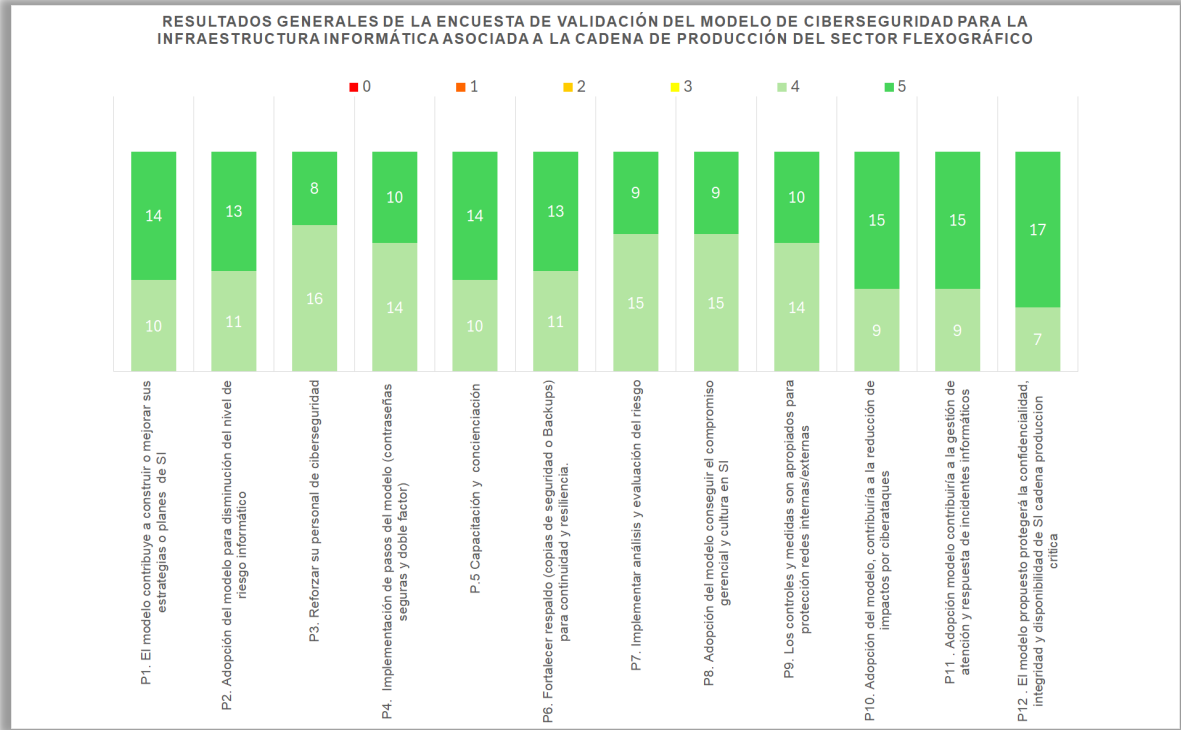


Fig. 16 Análisis de Pareto de los resultados obtenidos en la validación del modelo de ciberseguridad desarrollado para los sistemas TI vinculados a la gestión de la cadena de producción crítica de la industria flexográfica.

Nota: Como se observa, en contrario al diagnóstico inicial del sector, los riesgos se han reducido significativamente mediante el modelo de ciberseguridad para los sistemas TI vinculados a la gestión de la cadena de producción crítica de la industria flexográfica. Fuente: Autoría propia.

En efecto y como se recordará, del análisis de Pareto producto del diagnóstico sectorial inicial (ver Fig.10), en general, las empresas de la industria flexográfica mostraban un nivel de madurez muy bajo, caracterizado por la implementación parcial o inexistente de controles esenciales, como contraseñas robustas, doble factor de autenticación, estrategias de copia de seguridad confiables, nula o bajísima capacitación del personal y ausencia de procesos estructurados basados en análisis y evaluación del riesgo y falencias sustanciales en sus estrategias de seguridad informática, reflejando un escenario en el que predominaban prácticas informales e incipientes, debilidades operativas y una limitada comprensión de la importancia estratégica de la seguridad informática para la continuidad del negocio y para la integridad de la cadena de producción.

En contraste, el nuevo análisis final de Pareto, mostrado en la Fig. 17, presenta una concentración de respuestas en niveles altos de aceptación (valores 4 y 5 en la escala de Likert) y este comportamiento indica que, las organizaciones consultadas, reconocen la utilidad, pertinencia, efectividad, eficacia y viabilidad del prototipo cibernético protectivo desarrollado, pues, en efecto, controles y prácticas que inicialmente presentaban bajas tasas de adopción, como, por ejemplo, el fortalecimiento de la autenticación, la gestión de respaldos, la capacitación especializada y el análisis formal del riesgo, ahora son percibidos como necesarios y adecuados para las compañías.

Adicionalmente, vale resaltar que, las compañías encuestadas, valoran positivamente la capacidad del nuevo modelo cibernético de protección desarrollado para contribuir a la reducción del impacto de los ciberataques, mejorar la continuidad operativa, apoyar la toma de decisiones y reforzar la confidencialidad, la integridad y la disponibilidad de la seguridad de la información y, en especial aprecian el robustecimiento de la resiliencia de la infraestructura informática crítica del sector flexográfico.

Esta transición demuestra un cambio conceptual importante, despertado en el sector por el solo hecho de indagar sobre ciberseguridad y que fue logrado y afianzado con el sometimiento a consideración del modelo de ciberseguridad desarrollado a la propia industria flexográfica. En particular, vale destacar que, el nuevo marco CCCI en que se fundamenta y que sirvió de herramienta pedagógica, didáctica y técnica para explicar el prototipo cibernético protectivo, sirvió y fue muy útil para plantear los conceptos complejos de la ciberseguridad entre el personal de producción sectorial.

De otra parte, también se destaca que, mientras en el diagnóstico inicial predominaba una postura reactiva frente a la ciberseguridad de parte del sector flexográfico, en total contraste, los resultados obtenidos de la verificación y validación del prototipo cibernético protectivo confirman una actitud favorable hacia la adopción de un enfoque más proactivo, sistemático, holístico y alineado con los estándares internacionales y las mejores prácticas de ciberseguridad de parte de la industria.

En síntesis, el contraste en los análisis de Pareto confirma que el modelo de ciberseguridad propuesto responde directamente a las debilidades identificadas en el diagnóstico inicial y que, su enfoque integral es valorado como oportuno y necesario por la industria flexográfica, puesto que, la validación realizada no solo legitima la pertinencia del prototipo protectivo en términos conceptuales, sino que, también, muestra una mayor conciencia y sensibilización sobre la importancia de fortalecer los pilares organizacionales de la ciberseguridad como fundamento para la protección, estabilidad, continuidad y resiliencia de la cadena productiva flexográfica.

Consecuentemente, con base en los resultados obtenidos en la actividad 3.3, se volvieron a elaborar unos nuevos autodiagnósticos de estado final y una nueva matriz de riesgos y su respectivo mapa de calor de estado final. Estas nuevas herramientas se basaron en los resultados obtenidos de la aplicación del instrumento (encuesta final de verificación, actividad 3.2) a fin de poder determinar la reducción del nivel de riesgo para la infraestructura informática vinculada a los procesos productivos críticos sectoriales, obtenido con la consideración del modelo de ciberseguridad desarrollado de parte de la industria flexográfica. Estos resultados se muestran en los Anexos Nros. 9 y 10 de esta tesis de maestría.

En conclusión, entre los resultados más relevantes de la fase 3.3 se tiene que el modelo de ciberseguridad propuesto para la protección de la confidencialidad, la integridad y la disponibilidad de infraestructura informática de la cadena productiva de las PYMEs y empresas de la industria flexográfica responde con efectividad y eficacia a las especificidades protectivas, tecnológicas y organizacionales que requiere el sector, y cuyos aspectos más importantes pueden agruparse en cinco (5) ejes fundamentales: reducción de riesgos, concienciación y capacitación del personal, continuidad y resiliencia, cumplimiento normativo y conservación de la confidencialidad, integridad y disponibilidad (triada de la CIA). A continuación, se observan cada uno de ellos en mayor detalle, a saber:

4.3.1.4.1. Reducción significativa de riesgos informáticos

En este sentido, y siguiendo las recomendaciones de [25], se elaboró una comparación entre los resultados del mapa de aceptabilidad del riesgo informático sectorial de la infraestructura TI resultante del diagnóstico inicial del estado de la seguridad de la información en el sector flexográfico y los resultados finales derivados de la verificación y validación del modelo de ciberseguridad, lo cual arrojó una mejora significativa en la posición de ciberseguridad y una reducción sustancial del riesgo cibernético. Sin embargo, esto no demerita la necesidad de implementar, en un trabajo futuro, la protección de los sistemas OT.

A este respecto, el análisis inicial evidenció que las PYMEs y empresas del sector flexográfico enfrentan un panorama de riesgo cibernético complejo, donde se destacan múltiples ciberamenazas, en particular, la ingeniería social (especialmente phishing), el ransomware y el malware, sin embargo, la validación del modelo de ciberseguridad desarrollado permitió establecer que, se logra una reducción significativa del nivel de riesgo y una reducción apreciable de la superficie de exposición, gracias a la integración de controles de protección y estrategias de defensa, lo que, para el caso se traduce en una mejora de la postura de seguridad frente a escenarios críticos, como ciberataques, fallas tecnológicas o desastres.

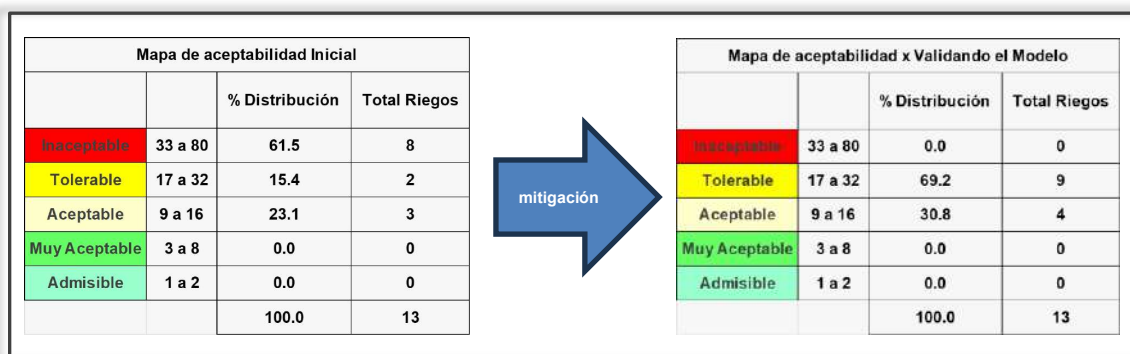


Fig. 17 Reducción significativa de riesgos cibernéticos obtenida con la consideración de modelo de ciberseguridad para los sistemas TI de la industria flexográfica y confirmada mediante la respectiva prueba conceptual de validación.

Nota: Como se observa, los riesgos más críticos disminuyen sustancialmente con el modelo de ciberseguridad desarrollado para los sistemas TI y considerado por la industria flexográfica. Fuente: Autoría propia.

Respecto a la aceptabilidad del riesgo derivada del modelo de ciberseguridad, como se muestra en la Fig. 17, se revela que los riesgos inaceptables se reducen de ocho (8) a cero (0), con mejoría de cien por ciento (100%) en protección y, en el aparte de los riesgos tolerables, estos aunque aumentan, producto del desplazamiento de todos los riesgos inaceptables, terminan en nueve (9), con mejoría general del sistema TI aunque no particular en este renglón específico de riesgos. El mapa de la aceptabilidad del riesgo final para los sistemas TI estudiados, anteriormente mostrados en la Fig. 17, también, se pueden apreciar en mayor detalle en el Anexo Nro. 10.

De otra parte, la identificación de los activos más sensibles, como, especialmente, los servidores de bases de datos y sistemas de respaldo que, obligadamente requieren medidas avanzadas de cifrado, redundancia y seguridad física, contribuyen a mejorar la ciberdefensa en profundidad, pues, la validación del modelo de ciberseguridad desarrollado, también, confirmó que el factor humano constituye un vector de riesgo central, lo que refuerza la necesidad de reforzar la capacitación y los controles de acceso, como indica la validación realizada.

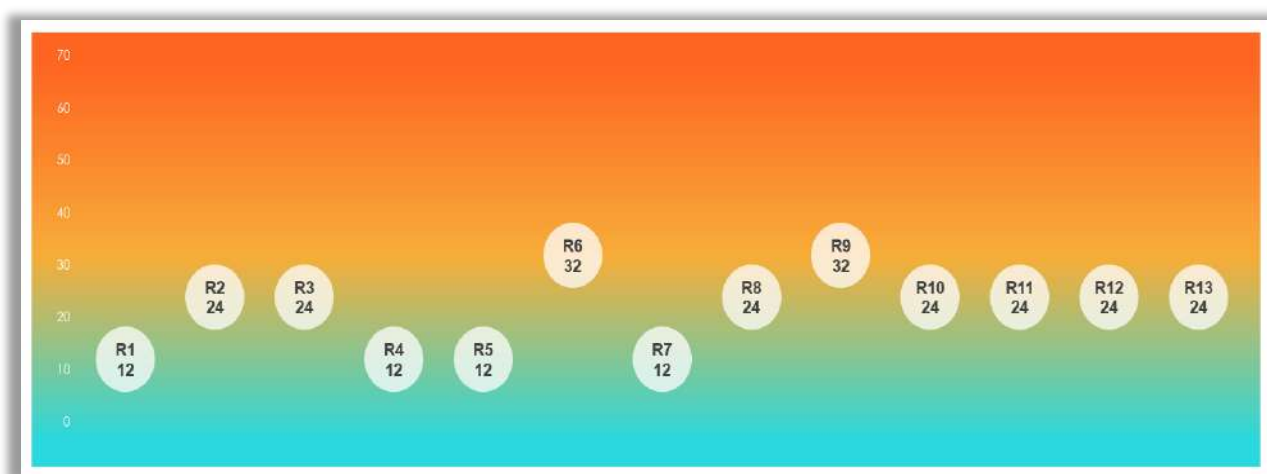


Fig. 18. Mapa de calor final obtenido con la consideración del modelo de ciberseguridad para los sistemas TI asociados a la gestión de los procesos OT de la cadena de producción crítica de la industria flexográfica.

Nota: La distribución de riesgos es muchísimo más benigna con la consideración del prototipo cibernético protectivo desarrollado para la defensa de la infraestructura TI de la industria flexográfica. Fuente: Autoría propia.

Complementariamente, la validación del modelo de ciberseguridad desarrollado, a través de sus estrategias de defensa y protección, consolidadas mediante controles específicos requeridos, logra la mitigación del riesgo de ciberamenazas como, por mencionar algunas, la ingeniería social (en particular, del phishing), el ransomware, el malware y la intrusión, todos, muy ampliamente identificados como ciberamenazas constantes y crecientes, tanto en sofisticación como en frecuencia, para el sector flexográfico, lo cual se traduce en una mejora sustancial de la posición de ciberseguridad, tal como muestra el mapa de calor consignado en la Fig. 18 y en más detalle en el Anexo Nro. 10 de esta tesis de maestría.

Sin embargo, debe tenerse en cuenta que, hasta este punto, acorde al objetivo general establecido en esta tesis de maestría, solo se ha realizado la mitad del esfuerzo de aseguramiento y que, la protección brindada por el modelo de ciberseguridad para los sistemas TI representan solamente la mitad de la labor de ciberdefensa necesaria, razón por la que, toda compañía deberá atender la protección de su infraestructura OT, no incluida en el presente trabajo de investigación, en razón a motivos del alcance metodológico definido.

4.3.1.4.2 Concienciación, capacitación y actualización permanente del personal corporativo

Los hallazgos revelaron que, existe una brecha crítica en la concientización y capacitación del personal, incluidos directivos, mandos medios y personal de planta. Estos resultados demuestran que la estrategia actual ha descuidado el factor humano como el eslabón más vulnerable de la cadena de la seguridad informática. En consecuencia, se evidencia la necesidad imperante de implementar un programa de formación continua, que puede ser basado en el marco CCCI que se presentará a continuación, de tal manera que trascienda la instrucción técnica y fomente una cultura de ciberseguridad proactiva capaz de mitigar riesgos cibernéticos y cobrar papel activo en la responsabilidad colectiva de protección digital.

4.3.1.4.3. Continuidad y resiliencia operacional.

El modelo de ciberseguridad propuesto, también, demostró su eficacia y efectividad para asegurar la continuidad del negocio y la resiliencia de las operaciones frente a incidentes tecnológicos o ante ataques cibernéticos, pues, gracias a la implementación de planes de contingencia, esquemas de respaldo redundante y otros controles, las empresas pueden recuperar sus sistemas críticos en tiempos aceptables, sin pérdida significativa de datos. El aporte de lograr un restablecimiento rápido de los sistemas TI se complementa con la capacidad de adaptación y ajuste que desarrollan las compañías con la implementación del modelo de ciberseguridad propuesto en esta tesis de maestría.

4.3.1.4.4. Cumplimiento normativo y legal.

Otro de los aspectos relevantes que aporta el modelo de ciberseguridad propuesto es que no se limita al plano técnico, sino que, complementariamente, se alinea con estándares y marcos regulatorios y normativos internacionales, fortaleciendo la gobernanza digital, lo cual lleva a que su eventual adopción asegure el cumplimiento legal exigido de los controles derivados de la norma ISO 27001, la integración de los pilares del marco NIST 2.0 CSF y la aplicación priorizada e inteligente de los CIS Controls. Esto se traduce en una mayor facilidad de superar procesos de auditorías y demostrar compromiso frente a clientes, proveedores y autoridades y, lo más importante, proteger mejor la infraestructura productiva crítica de las empresas.

En este contexto, el alineamiento y sincronía entre lo técnico y lo normativo, favorece la defensa en profundidad de la infraestructura informática y computacional asociada a la gestión de la cadena de producción crítica de la industria flexográfica, contribuyendo no solo a la reducción de brechas técnicas de naturaleza cibernética, pues, a través de la incorporación de estándares internacionales ampliamente aceptados y reconocidos, pone a las organizaciones en una mejor posición para cumplir con las exigencias de los

marcos legales y, también, en condiciones óptimas, para enfrentar revisiones y auditorías de aspectos regulatorios y legales de sus mercados y, todo, mientras se gestionan adecuadamente los riesgos cibernéticos asociados a terceros y se demuestra ante clientes, proveedores y potenciales interesados, el compromiso organizacional con la seguridad digital y con la obediencia de la Ley.

En particular, el modelo de ciberseguridad propuesto no solo actúa como una mera guía técnica, sino que, también, constituye una herramienta de cumplimiento para el marco legal y jurídico obligatorio de Colombia, pues, su implementación satisface las normativas de la Ley 1581 de 2012 de protección de datos personales, obligando a las empresas a adoptar medidas técnicas y administrativas para evitar el acceso no autorizado o la pérdida de información.

Asimismo, la estructura del prototipo cibernético propuesto se alinea con la Ley 1273 de 2009 de Ley de Delitos Informáticos, al establecer protocolos de protección que ayudan y contribuyen a la protección de la confidencialidad, la integridad y la disponibilidad de los activos digitales, previniendo conductas penales como el daño informático o el acceso abusivo. De otra parte, el esquema propuesto, también, responde a las nuevas exigencias de la Ley 2502 de 2025 sobre uso malintencionado de inteligencia artificial (AI) ya vigente y del espíritu que orienta al proyecto de Ley que introduce el concepto de ciberseguridad activa, exigiendo monitoreo en tiempo real para mitigar riesgos en un entorno digital cada vez más sofisticado.

4.3.1.4.5. Conservación y aseguramiento de la confidencialidad, la integridad y la disponibilidad de la infraestructura informática vinculada al soporte de los procesos OT de la cadena de producción esencial de la industria flexográfica.

Finalmente, el modelo fomenta el robustecimiento de la conservación y ciberprotección de los principios de confidencialidad, integridad y disponibilidad en los sistemas informáticos de las PYMEs de la industria flexográfica (e industrias esenciales similares). La confidencialidad e integridad se fortalecen

con trazabilidad y segregación de funciones, mientras que, la disponibilidad de los sistemas TI se asegura mediante redundancia, monitoreo en tiempo real y planes adecuados de recuperación.

Así pues, los mecanismos anteriores consolidan una protección efectiva a la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica que, además de reducir riesgos, contribuye a la competitividad empresarial, a la optimización de recursos y a la generación de confianza en clientes y terceros, puesto que la mitigación del riesgo y la reducción de la superficie de exposición ante ciberataques beneficia a la industria y genera confianza en terceros.

4.3.1.4.6. Aseguramiento y protección de la infraestructura OT de la cadena de producción crítica sectorial como tarea futura necesaria e indispensable para completar este modelo de ciberseguridad.

Como fue definido desde el alcance metodológico, será necesario, para las compañías del sector flexográfico, emprender la gestión protectiva futura de sus tecnologías e infraestructura OT, así como los sistemas de control industrial de sus cadenas de producción críticas, a fin de completar el esfuerzo de aseguramiento iniciado en esta tesis de maestría. Los lineamientos correspondientes se presentarán más adelante en el aparte de trabajos futuros.

4.3.2 Nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI)

De otra parte, y como destacado valor agregado de los resultados obtenidos en esta tesis de maestría en seguridad informática, es importante resaltar la creación del nuevo marco CCCI, ideado como una herramienta estratégica, pedagógica y técnica de apoyo para la ciberseguridad industrial. Al respecto, debe resaltarse que, el nuevo marco CCCI cubre nuevas dimensiones de seguridad informática que van orientadas al entorno de las industrias esenciales con cadenas productivas críticas como el sector flexográfico y que incluye nuevas dimensiones, adicionadas a la idea original de McCumber, como la

continuidad y la resiliencia, la implementación operativa (Adaptabilidad y flexibilidad, Integrabilidad e interoperabilidad, y escalabilidad) y los propios estándares y referentes internacionales de amplia aceptación que guían esta tesis de maestría.

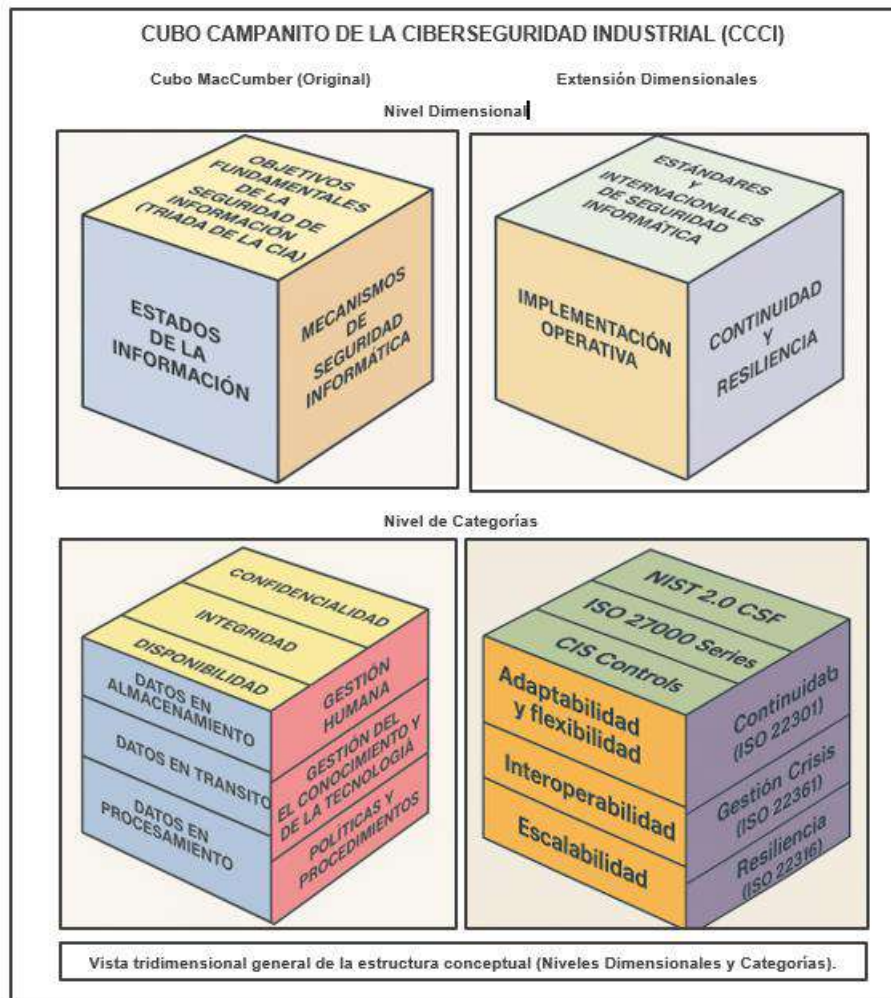


Fig. 19. Representación tridimensional completa del nuevo marco CCCI. Versión completa.

Nota: Industrial Cybersecurity Tinker Bell Cube (ICTBC) framework). Fuente: Tomado de [46]. Autoría propia.

El nuevo marco CCCI fue muy bien acogido por la industria flexográfica y por el público del sector académico de los eventos en que se presentó durante el último semestre de 2025, en razón a su calidad de constituir una gran herramienta de ayuda, no solo para la fácil asimilación conceptual, sino, también, como guía de orientación estratégica para la implementación, construcción y entendimiento de una arquitectura de ciberseguridad adaptada a la gestión de los riesgos actuales y

las necesidades propias de la industria, como para el caso, la flexográfica y, en especial, para PYMEs.

Como puede observarse en la vista tridimensional de la Fig. 19, el desarrollo del marco CCCI incluye: seis (6) dimensiones protectivas y diez y ocho (18) diversas categorías de actividades. También, se destaca el aporte original de McCumber [59] y el mejoramiento realizado, mediante la aplicación del proceso ingenieril de innovación, con la adición de las tres (3) nuevas dimensiones y sus respectivas categorías complementarias. Asimismo, el nuevo marco CCCI es detallado a profundidad en el Anexo Nro. 11 de esta tesis de maestría en seguridad informática.

Complementariamente, vale apuntar que, el CCCI en su función de herramienta de capacitación, sensibilización y concienciación, presenta una naturaleza dual, pues la implementación de este innovador enfoque estratégico, también, permitió identificar y priorizar las funciones críticas índole técnica de la infraestructura IT asociada a la cadena de producción de las empresas, y facilita la definición de medidas específicas para proteger la información, los sistemas de control, los activos digitales y las comunicaciones, mientras que, igualmente, ofrece un marco de referencia para evaluar el grado de madurez en ciberseguridad, orientar inversiones, justificar decisiones ante la alta dirección y cumplir con requerimientos regulatorios o contractuales, cada vez más frecuentes en entornos industriales permanentemente interconectados y expuestos a ciberamenazas.

Además, el CCCI reveló su gran potencial como marco pedagógico y didáctico, que permite facilitar la visibilización, comprensión, mejor entendimiento y asimilación del modelo de ciberseguridad desarrollado, tanto por parte de los gerentes y altos directivos, como también, del personal no especializado de las organizaciones y empresas flexográficas (operadores, personal de planta, etc.). Al efecto, el nuevo marco CCCI, cuya primera presentación en sociedad se realizó en la edición ciento diez y seis (ed. 116) de octubre de los corrientes, en la revista institucional La Tekné, publicada por el Fondo Editorial de I.T.M. [49], se presenta, en completo detalle, en el Anexo Nro. 14, junto con otros productos derivados de esta tesis.

Es importante mencionar que, este nuevo marco y lo desarrollado en este trabajo investigativo fue presentado en el Simposio Nacional de Maestrías y Doctorados del 19vo Congreso Colombiano de Computación de la Sociedad Colombiana de Computación y la Universidad Militar Nueva Granada (SNMyD25, 19CCC, SCo2 - U.M.N.G.) [23] y, también, la XX Conferencia Latinoamericana de Tecnologías de Aprendizaje [24] cuyas memorias se publicaran en el libro de Springer “*Lecture Notes in Computer Science*” de abril de los corrientes [24].

De otra parte, también, es importante resaltar que el nuevo marco CCCI, que se puede apreciar en mayor detalle en el Anexo Nro. 11 en su calidad de herramienta estratégica de naturaleza técnica y pedagógica, también, puede ser utilizado, cuando se emprenda el trabajo futuro para el aseguramiento y la protección de la infraestructura OT de la industria flexográfica, necesario para completar este trabajo de investigación y los resultados y hallazgos de esta tesis de maestría.

5. Discusión y análisis de resultados

En primer lugar, se resalta que, por las razones ya expuestas derivadas de la delimitación metodológica establecida, el presente trabajo destaca la importancia de la integración del pensamiento crítico en la ciberseguridad industrial, la cual constituye un pilar estratégico para la resiliencia de las infraestructuras críticas productivas, como la industria flexográfica. Lo anterior, en franco reconocimiento que, mientras los modelos protectivos de TI priorizan la confidencialidad de los datos, los enfoques especializados, que incluyen sistemas OT (o modelos de madurez), como los comparados de autoría de [53] y [54], enfatizan la disponibilidad y la integridad de los procesos físicos, es decir, se enfocan en la protección sobre la propia maquinaria de la industria flexográfica, respecto a la cual y como se definió de inicio, no forman parte del alcance problemático de esta tesis, pero que, sin lugar a duda alguna, constituye elemento clave en la labor de protección cibernética. Esta distinción exige que no solo se dominen herramientas técnicas de defensa y ataque, sino que, se desarrolle una capacidad analítica más profunda para diagnosticar anomalías en sistemas, como las cadenas de producción, donde una decisión errónea puede derivar en daños materiales o paradas de planta costosas, en plena sincronía y alineación con la búsqueda de la mayor mitigación de riesgo posible para la cadena productiva sectorial.

Por otro lado, un modelo de ciberseguridad robusto debe contemplar el factor humano como un componente activo capaz de interpretar hechos, evaluar premisas implícitas y comunicar incidentes de forma precisa entre los niveles operativos y los sistemas de gestión empresarial, como el ERP o el EMS. En última instancia, las futuras líneas investigativas requerirán de un alto nivel de equilibrio entre la pericia técnica en redes industriales e infraestructura OT y una disposición crítica que permita transformar la información técnica soportada en el presente trabajo, en conocimiento estratégico para la toma de decisiones de diseño acertadas para lograr una completa cobertura y protección de la cadena de producción crítica de la industria flexográfica.

Sin embargo, los resultados obtenidos en la presente tesis de maestría en seguridad informática permiten establecer una lectura integral del estado de la ciberseguridad de la infraestructura TI asociada a la cadena de producción crítica de la industria flexográfica en las PYMEs de una industria esencial e importante, como lo es el sector flexográfico, y proponer un modelo de ciberseguridad para la protección de la confidencialidad, la integridad y la disponibilidad de la seguridad de la información de la infraestructura IT asociada a la gestión de la cadena productiva crítica de esta importante industria esencial. Igualmente, se revelaron los diversos retos y desafíos estructurales que, en cuanto a la ciberseguridad, enfrenta la industria flexográfica, en particular, frente a la protección de su infraestructura informática asociada a la cadena de producción crítica.

En particular, para los sistemas TI vinculados con los procesos productivos de la industria flexográfica se constató la existencia de una brecha de seguridad que, se traduce en un nivel de madurez muy bajo en ciberseguridad y, que se ve reflejada en la ausencia de procesos formales de gestión del riesgo cibernético, en la limitada documentación de activos y en la carencia de controles robustos de acceso, segmentación y monitoreo a los sistemas IT asociados a la gestión, operación y control de los procesos y cadena productivos, lo cual configura un escenario de vulnerabilidad operacional para una industria, hoy por hoy, altamente dependiente de sistemas digitales y con equipos de impresión asistidos por software e interconectados al ciberespacio y a redes externas que dificultan la labor de protección cibernética y de gestión de defensa corporativa.

Esta exposición al riesgo cibernético es cubierta y solventada con propiedad por el modelo de ciberseguridad propuesto en esta tesis, pues, con base en su sometimiento a consideración de la industria y los resultados obtenidos de la validación realizada se hace notar que el modelo propende con eficacia y efectividad a la protección de la triada de la CIA de la seguridad de la información de los sistemas computacionales de la industria flexográfica y que, igualmente, podría ser aplicable en otros sectores esenciales con similares características y cadenas de producción críticas.

Un hallazgo destacado es la disonancia entre la percepción de riesgo de los responsables de las infraestructuras IT y la implementación efectiva de controles

técnicos y administrativos que, ahora, el modelo de ciberseguridad propuesto en esta tesis, entra a solventar, pues, mientras una parte significativa de los encuestados manifiesta reconocer la importancia de la ciberseguridad, los datos obtenidos en los resultados demuestran que la adopción de medidas concretas, como, por ejemplo, contraseñas seguras, autenticación multifactor, hardening de sistemas operativos y servidores, políticas de acceso fuertes, copias de seguridad verificables y controles de acceso basados en roles, sigue siendo parcial o inexistente. En este sentido, tanto el modelo de ciberseguridad desarrollado, como el nuevo marco CCCI en que fue inspirado, aportan decisivamente al mejoramiento de este aspecto y al mejoramiento de la ciberdefensa.

De otra parte, también, se observó la existencia de una brecha de seguridad, decantada entre la disyuntiva de la intención y acción, pues, los resultados obtenidos indican claramente que, el sector no solo enfrenta limitaciones técnicas y presupuestales, sino, también, vacíos en la cultura cibernética a nivel organizacional, pues la gobernanza digital y la priorización estratégica de la seguridad de la información, solo se atiende de manera parcial (o, incluso, se ignora) en una gran mayoría de PYMEs del sector (en este punto, se debe hacer la salvedad que, también hay, algunas pocas compañías grandes que gestionan muy bien su ciberseguridad, pero, que no constituyen un porcentaje apreciable o mayoritario entre las empresas del sector flexográfico).

En cuanto al análisis comparativo entre el diagnóstico inicial y el estado final, realizado mediante el sometimiento conceptual del modelo de ciberseguridad diseñado, se observa una mejora significativa en la capacidad sectorial para gestionar la ciberseguridad, incluyendo reducción de la superficie de exposición, respuesta a ciberincidentes y aumento de la resiliencia operativa, lo cual se traduce en una mejor ciberprotección. La integración de elementos del nuevo marco CCCI (presentado en detalle en el Anexo Nro. 11), que incluye estándares internacionales de ciberseguridad analizados en este trabajo, permite estructurar un enfoque híbrido que atiende los requerimientos cibernéticos reales de las empresas, especialmente, la necesidad de controles mínimos, progresivos y auditables, mientras que facilita la asimilación y adopción del modelo de ciberseguridad por parte de las empresas del sector, aunado el fomento de la cultura de la ciberseguridad.

Complementariamente, el modelo de ciberseguridad diseñado plantea una secuencia gradual de implementación que inicia con la gestión del riesgo basado en la identificación de activos críticos y avanza hacia la formalización de políticas y estrategias de ciberseguridad que serán posteriormente implementadas mediante controles técnicos esenciales y el desarrollo de capacidad de ciberprotección avanzadas, como la respuesta a incidentes, el monitoreo constante, el mejoramiento continuo del propio prototipo cibernético protector. Sin embargo, las empresas no necesariamente deben continuar de manera obligada con el establecimiento de capacidades avanzadas, pues la flexibilidad es una de las características del modelo de ciberseguridad propuesto.

En este contexto, la verificación de la eficacia y efectividad del modelo de ciberseguridad desarrollado y su validación, realizada mediante prueba conceptual (encuesta de verificación) confirmó que la integración metodológica propuesta es pertinente, factible y adaptable a estructuras organizacionales como las que caracterizan a las PYMEs del sector flexográfico (y, potencialmente, a otras industrias esenciales con cadenas productivas críticas y características similares), donde los roles de los miembros del equipo corporativo suelen estar concentrados y los recursos de inversión en soluciones tecnológicas son extremadamente limitados.

Completando lo anteriormente disertado, es importante destacar que, dentro de los resultados obtenidos del proceso investigativo de esta tesis de maestría, se ha creado el nuevo marco CCCI, el cual ha surgido como producto de un proceso ingenieril de innovación, realizado mediante el mejoramiento, expansión, complementación, adaptación y actualización del cubo de McCumber de la seguridad informática que, ha de servir para orientar las labores técnicas de la ciberseguridad industrial y, simultáneamente, para facilitar la visibilización, el entendimiento, comprensión y asimilación de los conceptos técnicos, en su función pedagógica y didáctica, propugnando por una más fácil adopción de parte de la industria de los modelos de ciberseguridad que con su fundamento puedan generarse.

De otro lado, la discusión sobre los resultados obtenidos confirma que la adopción de un enfoque estructurado, basado en estándares internacionales, resulta esencial para

elevar la resiliencia digital del sector flexográfico. Así pues, la innovadora consolidación del nuevo marco conceptual CCCI derivado del mejoramiento del cubo de McCumber y su adaptación al contexto de industrias esenciales con cadenas de producción críticas demuestran su valía, al constituir una novedosa metodología útil, tanto desde lo meramente técnico, como desde la perspectiva pedagógica y didáctica, para integrar dimensiones estratégicas, industriales, tecnológicas y operacionales en un solo framework aplicable. La visión multidimensional del CCCI permite generar un marco robusto, coherente y adaptable a las necesidades de sectores productivos e industrias esenciales.

Así pues, vale decir que los resultados de esta tesis de maestría en seguridad informática evidencian que, aunque el sector flexográfico presenta rezagos significativos en ciberseguridad, existe un camino claro y viable hacia el mejoramiento de la seguridad informática, siempre y cuando se articulen estrategias de gestión, inversión progresiva, capacitación continua y adopción disciplinada de controles, como los propuestos en el modelo de ciberseguridad desarrollado para esta industria esencial. Y sin olvidar, que, este camino pasa, por la protección de los sistemas OT.

De otra parte, finalizando las presentes disertaciones, y en aras de contribuir a trabajos futuros para el aseguramiento y protección de la infraestructura OT, a continuación, se realiza un comparativo entre el trabajo efectuado y las contribuciones de Villa [53] y Caro [54] que, si lo han incluido en sus respectivos sectores, a saber:

- En primer lugar, se resalta que, por las razones ya expuestas derivadas de la delimitación metodológica establecida, el presente trabajo destaca la importancia de la integración del pensamiento crítico en la ciberseguridad industrial, la cual constituye un pilar estratégico para la resiliencia de las infraestructuras críticas productivas, como la industria flexográfica. Lo anterior, en franco reconocimiento que, mientras los modelos protectivos de TI priorizan la confidencialidad de los datos, los enfoques especializados, que incluyen sistemas OT (o modelos de madurez), como los comparados de autoría de [53] y [54], enfatizan la disponibilidad y la integridad de los procesos físicos, es decir, se enfocan en la protección sobre la propia maquinaria de la industria flexográfica, respecto a la cual y como se definió de inicio, no forman parte del

alcance problemático de esta tesis, pero que, sin lugar a duda alguna, constituye elemento clave en la labor de protección cibernética. Esta distinción exige que no solo se dominen herramientas técnicas de defensa y ataque, sino que, se desarrolle una capacidad analítica más profunda para diagnosticar anomalías en sistemas, como las cadenas de producción, donde una decisión errónea puede derivar en daños materiales o paradas de planta costosas, en plena sincronía y alineación con la búsqueda de la mayor mitigación de riesgo posible para la cadena productiva sectorial.

- Por otro lado, un modelo de ciberseguridad robusto debe contemplar el factor humano como un componente activo capaz de interpretar hechos, evaluar premisas implícitas y comunicar incidentes de forma precisa entre los niveles operativos y los sistemas de gestión empresarial, como el ERP o el EMS, como se propone en [23], [24] y [49]. En última instancia, las futuras líneas investigativas requerirán de un alto nivel de equilibrio entre la pericia técnica en redes industriales e infraestructura OT y una disposición crítica que permita transformar la información técnica soportada en el presente trabajo, en conocimiento estratégico para la toma de decisiones de diseño acertadas para lograr una completa cobertura y protección de la cadena de producción crítica de la industria flexográfica.

6. Consideraciones finales

Este esfuerzo de aprendizaje e investigación consolida algunos dictámenes y lecciones importantes a la luz del análisis integral de los marcos normativos internacionales, las buenas prácticas de seguridad informática y los principios fundamentales de protección de la información, en la labor de diseño de un modelo de ciberseguridad orientado a la protección y al aseguramiento de la confidencialidad, la integridad y la disponibilidad de la infraestructura IT asociada a la gestión, control y operación de la cadena de producción de una PYME o empresa de la industria flexográfica, pues permite avanzar hacia un entorno más confiable, resiliente y operativo. A continuación, las principales conclusiones, recomendaciones, lecciones aprendidas y trabajos futuros que se derivan de esta tesis de maestría en seguridad informática:

6.1 Conclusiones

A continuación, se plantean algunas conclusiones derivadas de este esfuerzo investigativo y que, a saber, son las siguientes:

La principal conclusión de esta tesis de maestría en seguridad informática consiste en evidenciar que, aun en organizaciones con recursos limitados y con una madurez cibernética inicial muy baja, es posible establecer un modelo de ciberseguridad cibernética para los sistemas TI que, a través de un conjunto seleccionado de controles estratégicos y tácticos, con fundamento en referentes y estándares internacionales de amplia aceptación, contribuyan al mejoramiento de la protección y defensa de la seguridad de la información, de manera progresiva, flexible, paulatina, adaptable y personalizable, acordes con las condiciones particulares de cada empresa y sin perjuicio del adecuado, eficaz y efectivo aseguramiento y conservación de la confidencialidad, la integridad y la disponibilidad de los activos e infraestructura informática asociada a su

cadena de producción crítica. Deberán, los trabajos futuros, incluir la protección y aseguramiento de las infraestructuras OT, no tratadas en la presente por cuestiones de alcance metodológico en esta tesis de maestría, pero, de obligatorio y necesario mandato, para lograr la completa ciberdefensa de las cadenas productivas críticas del sector flexográfico.

El trabajo investigativo evidenció que las PYMEs y empresas del sector flexográfico operan en un entorno de riesgo cibernético elevado, donde la madurez inicial en ciberseguridad es baja y predominan brechas como la ausencia de estrategias formales de seguridad informática, a lo cual se adiciona un alto nivel de exposición al riesgo, bajísima capacitación y pocos conocimientos en el tema, controles de acceso extremadamente débiles. Adicionalmente, se identificó que los activos más críticos (servidores de bases de datos y sistemas de respaldo) presentan niveles de riesgo "alto y muy alto" frente a ciberamenazas, como ingeniería social, ransomware, malware, entre otros. El análisis de riesgo confirmó que la continuidad operativa de la cadena de producción crítica no depende solo de la maquinaria industrial, sino, también, de la robustez de la infraestructura informática que la soporta y gestiona, siendo el factor humano y la obsolescencia tecnológica algunos de los puntos de mayor vulnerabilidad.

Por lo anterior, y en un entorno donde las guías de ciberseguridad suelen ser teóricas, pero, poco contextualizadas, otro hallazgo significativo es la correspondencia presente entre la adopción e implementación del modelo de ciberseguridad desarrollado y la reducción de las brechas existentes de ciberseguridad sectorial, previamente identificadas, particularmente en el caso de las PYMEs. A este respecto, además de las vulnerabilidades anteriores, también, se identificaron otras falencias preocupantes, como carencias de segmentación de redes, inexistencia de monitoreo centralizado continuo y en tiempo real, ausencia de planes de contingencia, falta de documentación relevante y bajos niveles de respaldo, ausencia de mecanismos de recuperación, entre otros, razones por las cuales, tras considerar la aplicación del modelo de protección cibernética propuesto, la mayoría de estas brechas lograron mitigarse parcial o completamente reduciendo de manera significativa el nivel de riesgo sectorial, aspecto que valida empíricamente la efectividad y eficacia del prototipo cibernético protectivo desarrollado.

La validación del prototipo cibernético protector efectuado mediante una prueba conceptual concretada en la aplicación de la encuesta de verificación demostró una aceptación general y completa en sus niveles de pertinencia y viabilidad, con excelentes resultados que confirman que el modelo de ciberseguridad propuesto para la infraestructura TI, constituye una solución útil y práctica y que responde con efectividad y eficacia a las necesidades sectoriales, logrando mitigar las brechas identificadas en el diagnóstico inicial y logrando una significativa reducción del riesgo informático.

De otra parte, otro gran aporte del modelo de ciberseguridad propuesto para la infraestructura TI asociada a la cadena de producción crítica del sector en estudio, es lograr la transición de un estado de ciberprotección reactiva a un estado de defensa en profundidad proactivo, lo cual fue reconfirmado mediante el análisis de Pareto y los mapas de calor y de aceptabilidad del riesgo elaborados con base en los resultados de la prueba conceptual de validación (encuesta de verificación), que mostraron una reducción significativa en la superficie de exposición y una mejora sustancial en la postura de seguridad de los sistemas TI, tras la aplicación de los controles estratégicos propuestos por el modelo de ciberseguridad desarrollado para la infraestructura TI asociada a la cadena de producción crítica del sector flexográfico.

A este efecto, el análisis de las respuestas obtenidas en la fase de validación del modelo de ciberseguridad propuesto, se evidencia una tendencia clara y consistente respecto a que, todas las organizaciones encuestadas valoran altamente la pertinencia, utilidad e impacto del prototipo cibernético protector propuesto para la mejora de su postura de seguridad informática. En cada una de las preguntas evaluadas, desde construcción de estrategias, disminución del riesgo informático, fortalecimiento del personal especializado e implementación de controles, adopción de la capacitación permanente en ciberseguridad, entre otros aspectos fundamentales, los resultados reflejaron la efectividad y eficacia para la protección de la confidencialidad, integridad y disponibilidad de la seguridad de la información, lo cual se traduce en una aceptación completa del modelo de ciberseguridad desarrollado y de sus recomendaciones.

Como logro y resultado de valor agregado se propuso una arquitectura modular y de bajo costo basada en el nuevo marco CCCI, una evolución innovadora del Cubo de

McCumber que integra de forma armónica las dimensiones protectivas que requiere la industria actual. Su diseño está especialmente orientado a PYMEs, ya que permite una implementación progresiva que prioriza la continuidad del negocio y la resiliencia digital operativa mediante los estándares internacionales analizados, asegurando que la ciberdefensa no se convierta en un obstáculo sino, en contrario, en una labor proactiva y preventiva. El hallazgo fundamental de esta propuesta es que la eficacia técnica del modelo para la infraestructura TI depende de trascender los bits y bytes para enfocarse en el componente humano donde cobra mayor relevancia el marco CCCI; así, mediante una cultura de corresponsabilidad, capacitación y mejora continua, se logra que la seguridad de la información sea un sistema vivo y adaptable que garantice la tríada de la seguridad (CIA) y la sostenibilidad de la industria a largo plazo.

Debe resaltarse que, el marco CCCI logra trascender la implementación técnica al alinear las medidas de seguridad con las dimensiones organizacionales, pedagógicas, funcionales y tecnológicas del entorno de las industriales reales. Al actualizar la concepción del cubo original de McCumber e integrar las nuevas dimensiones protectivas, el nuevo marco CCCI se posiciona como una herramienta de ciberdefensa en profundidad altamente versátil para el diseño de modelos cibernéticos protectivos particulares y, también, como guía orientadora y de capacitación. Finalmente, se resalta que la arquitectura dimensional del marco CCCI no es exclusiva para el sector flexográfico, sino que posee un alto potencial de transferencia y aplicación hacia cualquier otra industria esencial de la economía real con cadenas de producción críticas similares, consolidándose como un sistema integral de ciberprotección y ciberdefensa.

6.2 Recomendaciones

A continuación, y resaltando de entrada, la necesidad de acometer trabajos futuros para la protección de los sistemas OT, se plantean algunas recomendaciones pertinentes para empresas del sector flexográfico, que valga resaltar, son extensibles y aplicables a otros sectores con cadenas productivas críticas de industrias igualmente esenciales y que, a saber, son:

La primera recomendación es la adopción de un enfoque basado en riesgos que considere los activos informáticos críticos asociados a la gestión de la cadena productiva crítica de la industria flexográfica y, al respecto, se sugiere aplicar una metodología de análisis de riesgos como la propuesta por la norma ISO 27001 o, aún mejor, en la norma ISO 27005, en la que se identifiquen, valoren y prioricen los riesgos de acuerdo con su impacto sobre la confidencialidad, integridad y disponibilidad de la seguridad de la información de las infraestructuras TI vinculadas con los procesos productivos sectoriales. Este análisis debe considerar los flujos de datos en los tres (3) estados descritos en el nivel dimensional del estado de la información del cubo de McCumber (en reposo, en tránsito y en procesamiento) y vincularse a las funciones del marco NIST 2.0 CSF (gobernar, identificar, proteger, detectar, responder y recuperar) en su calidad de core o núcleo del modelo de ciberseguridad basado en el nuevo marco CCCI, pues de esta manera, el modelo podrá estructurarse no como un conjunto genérico de controles, sino, como un sistema de gestión centrado en la continuidad y la resiliencia operativa de los procesos más sensibles.

Específicamente, se recomienda iniciar con la gestión de inventarios de hardware y software, el control de cuentas y privilegios, la configuración segura de sistemas, la protección contra malware, y la implementación de copias de seguridad periódica de los datos. A ello debe añadirse la segmentación de red y el monitoreo de tráfico en tiempo real, como medidas prioritarias para entornos industriales que suelen tener conexiones vulnerables entre áreas internas (producción, administración, comercial, mercadeo, contabilidad, entre otros) y servicios externos, vía conexión permanente al ciberespacio.

En segundo lugar, la creación de una política de gobernanza de la seguridad de la información ya sea alineada con la norma ISO 27001 o con otro referente internacional de amplia aceptación y que, aunque no se trata necesariamente de un proceso de certificación en propiedad, sí constituye una basa fundamental que permite al modelo de ciberseguridad particular definir roles, responsabilidades y procesos de supervisión, aseguramiento y mejora continua. En este sentido, también, se recomienda la designación de un responsable interno de seguridad informática, aunque no se trate de un CISO formal u oficial y, además, realizar el establecimiento de un comité de ciberseguridad que integre representantes de distintas áreas de la compañía. Esto

permitirá institucionalizar las decisiones en materia de ciberseguridad, reducir la dependencia de soluciones reactivas y fomentar una cultura organizacional orientada a la protección de la información como activo estratégico de cada empresa.

Además, es esencial incluir una estrategia de formación y concienciación continua, como componente estructural del modelo propuesto y este aspecto, frecuentemente subestimado, es esencial para las industrias esenciales donde la operación diaria recae en personal que, si bien es altamente capacitado en los procesos productivos, puede carecer de conocimientos básicos en seguridad digital. A este respecto, el nuevo marco CCCI permite abordar esta dimensión mediante programas diferenciados de capacitación según roles y responsabilidades, simulacros de respuesta a incidentes, campañas internas de concienciación y la integración de la ciberseguridad en los procesos de inducción y evaluación de desempeño. La protección de la infraestructura IT no depende exclusivamente de gestión técnica, como configuración de firewalls u otros similares, sino de la capacidad de todos los actores involucrados para comprender, detectar y actuar frente a eventos de riesgo cibernético.

Una recomendación adicional se refiere a la adopción de medidas de monitoreo, respuesta y recuperación ante incidentes y, en este sentido, se sugiere desarrollar procedimientos operativos para la gestión de eventos de seguridad, incluyendo mecanismos de detección de anomalías, escalamiento de alertas y planes de recuperación de servicios críticos. Aunque en su gran mayoría, las organizaciones del sector flexográfico (en especial las PYMEs), no cuentan con equipos especializados (como un CSIRT interno), si es posible implementar soluciones adaptadas como alianzas con proveedores de servicios gestionados o la participación en redes de colaboración sectorial o con autoridades gubernamentales. En este sentido, el uso del marco NIST 2.0 CSF permite estructurar estas capacidades de forma modular, asegurando que incluso organizaciones con capacidades limitadas puedan adoptar mecanismos mínimos de defensa activa y restauración funcional ante incidentes de ciberseguridad.

Adoptar el marco CCCI como referente técnico, pedagógico y organizacional para gestionar la mejora continua y no solamente como una intervención técnica aislada, aprovechándolo como fuente de directrices estratégicas clave para aspectos

fundamentales de seguridad como la formación del personal, la actualización de políticas, la seguridad física y la gestión de riesgos. Su uso puede ser complementado, para incrementar la eficacia y la efectividad a largo plazo, con el uso de indicadores de madurez basados en los estándares internacionales analizados, junto con auditorías periódicas que permitan adaptar el sistema a los cambios tecnológicos y normativos del entorno industrial. Lo anterior en razón a que, ante la creciente digitalización de la industria real, como el sector flexográfico, la ciberseguridad deja de ser una opción netamente técnica para convertirse en un cimiento crítico de la supervivencia y la sostenibilidad corporativas en el ámbito de la economía real.

6.3 Lecciones aprendidas

El desarrollo de esta tesis de maestría permitió no solo el diseño de un modelo de ciberseguridad específico para las PYMEs de la industria flexográfica, sino, también, la identificación de valiosas lecciones aplicables al ámbito industrial, académico, profesional y organizacional. Estas lecciones constituyen un conjunto de aprendizajes que enriquecen la comprensión de la seguridad informática en sectores productivos críticos y sirven como referente para futuras investigaciones y aplicaciones prácticas.

- **Importancia de contextualizar la ciberseguridad al sector industrial**

Una de las principales lecciones aprendidas de este esfuerzo investigativo fue reconocer que las PYMEs de la industria flexográfica presentan características propias (limitaciones presupuestales, dependencia tecnológica creciente y procesos críticos de producción) que requieren modelos de seguridad adaptados a su realidad. No basta con aplicar estándares internacionales de forma genérica: es necesario traducirlos a soluciones viables, prácticas y económicas.

Es importante resaltar que, esta lección aprendida es extensible a otras industrias y sectores de la economía real con cadenas de producción críticas similares a la analizada en esta tesis de maestría en seguridad informática, donde el modelo de

ciberseguridad desarrollado para la infraestructura TI puede ser potencialmente adaptado, aplicado e implementado.

- **La gestión del riesgo informático como eje central de ciberdefensa**

El análisis y la evaluación del riesgo informático mediante inventario de activos, detección de amenazas, identificación de vulnerabilidades, construcción de tablas de probabilidad/impacto y mapas de calor demostraron que, la gestión del riesgo debe ser la columna vertebral de cualquier modelo de ciberseguridad efectivo y eficaz. La lección aprendida es que conocer con precisión qué proteger y cómo priorizar es más efectivo y eficaz que implementar controles aislados o improvisados. Se debe siempre propender por realizar la evaluación del riesgo informático como base para cualquier estrategia de ciberseguridad.

- **Valor de los estándares y marcos de referencia internacionales**

La revisión de estándares internacionales de amplia aceptación como los ya mencionados y referencia de este trabajo (normas ISO 27000 series, el marco NIST 2.0 CSF y los CIS Controls), aunada a la consideración de las mejores prácticas de seguridad informática, mostraron que constituyen una base sólida para estructurar estrategias de protección. Sin embargo, la lección aprendida clave fue que estos referentes requieren de ajustes, adaptación e integración, tanto con la realidad de las organizaciones, como para su funcionamiento y operación simultánea (entre sí) para poder responder adecuadamente ante condiciones específicas de empresas con recursos limitados, como es el caso particular de las PYMEs.

- **Necesidad de combinar lo técnico con lo humano y lo organizacional**

El proceso investigativo permitió evidenciar que la seguridad informática no depende únicamente de herramientas tecnológicas, sino de la capacitación del personal, las políticas organizacionales y la cultura de ciberseguridad. La lección fue clara: sin un componente humano robusto y consciente, los controles técnicos pierden eficacia. El eslabón más débil sigue y seguirá siendo el ser humano, por tal razón, es importante

involucrarlo en los procesos de ciberseguridad, tanto desde la capacitación, como desde la participación proactiva el involucramiento directo en la estrategia de protección cibernética.

- **Continuidad y resiliencia como objetivo estratégico**

Finalmente, otra lección aprendida consiste en que en un sector industrial esencial, como el flexográfico (o cualquier otro de la economía real) y, en particular, en el ámbito de las cadenas productivas críticas, la verdadera meta de la ciberseguridad no es únicamente prevenir ciberataques, sino fortalecer y robustecer la capacidad organizacional de continuidad operativa y de resiliencia organizacional, que serán las mejores bazas protectivas ante cualquier eventualidad: ciberataques, fallas técnicas, contingencias o desastres.

- **El valor de los procesos ingenieriles de innovación metodológica**

La extensión del cubo de McCumber hacia el nuevo marco CCCI representó un aporte innovador y útil para integrar continuidad, resiliencia y estándares internacionales dentro de un mismo marco conceptual haciendo la ciberdefensa más profunda e integral y con participación activa del componente humano. La lección aprendida es que los modelos clásicos deben evolucionar para responder a las nuevas realidades industriales y a los desafíos de la transformación digital.

Las lecciones aprendidas de esta investigación de tesis de maestría en seguridad informática destacan la importancia estratégica de la gestión del riesgo, la continuidad y la resiliencia como objetivos relevantes e irrenunciables; la integración de factores técnicos y humanos, el valor de los referentes, estándares y marcos normativos internacionales y, en especial, la importancia de la innovación conceptual y metodológica.

Estos aprendizajes fortalecen no solo el diseño del modelo de ciberseguridad planteado en esta tesis de maestría en seguridad informática, sino, también, la capacidad de la sociedad, en particular de las PYMEs del sector flexográfico (y otras similares de la economía real con cadenas de producción críticas) para enfrentar con mayor seguridad

y confianza los retos cibernéticos de la actual era digital en sus infraestructuras TI y, a futuro en la protección de sus procesos OT.

6.4 Trabajos futuros

A partir de esta tesis de maestría, que versa sobre el diseño de un modelo de ciberseguridad fundamentado en estándares internacionales y buenas prácticas de seguridad informática y basado en el CCCI, en su calidad de extensión del cubo de McCumber, y cuya orientación específica se enfoca en la protección de la infraestructura IT asociada a la gestión de la cadena productiva crítica de la industria flexográfica, se abren múltiples líneas de investigación futura con un alto valor académico, técnico y sectorial, que pueden ser acometidas por futuros maestrantes en seguridad informática o por estudiantes del postgrado en ciberseguridad.

Estas potenciales investigaciones futuras pueden contribuir a consolidar el conocimiento especializado en la protección de sectores productivos industriales, particularmente de infraestructuras críticas, en aras de fortalecer la resiliencia de PYMES y medianas empresas de los sectores industriales y, adicionalmente, a desarrollar marcos metodológicos replicables en otros entornos industriales (tecnológico, servicios, comercial, et al), pues la integración del enfoque extendido del cubo de McCumber, logrado en la creación del nuevo marco CCCI, permite, también, proyectar nuevos e interesantes estudios investigativos que trasciendan lo puramente técnico, para incorporar dimensiones organizacionales, humanas y contextuales, siempre fundamentales en el éxito de cualquier estrategia de ciberseguridad o de seguridad informática.

A continuación, algunas otras ideas para trabajos de investigación futura que se desprenden de esta tesis de maestría en seguridad informática, a saber:

-
- **Diseño de un modelo de ciberseguridad para la infraestructura OT asociada a la cadena de producción crítica de la industria flexográfica.**

Al efecto, una primera línea de investigación futura obligada consiste en completar la presente tesis de maestría en seguridad informática, incluyendo el diseño, bajo similares premisas, para la infraestructura OT asociada a los procesos de producción críticos de las PYMEs y empresas del sector flexográfico. Este enfoque permitirá evolucionar de una ciberdefensa básica hacia una resiliencia operativa de los procesos productivos capaz de mitigar aún más el riesgo cibernético, en especial, el que podrían comprometer la seguridad física de maquinaria y equipos, el suministro energético o la integridad de los procesos industriales críticos, que por alcance metodológico no fueron tratados en esta tesis de maestría en seguridad informática.

Al efecto el desarrollo protectivo para los sistemas OT deberá incluir similares etapas y establecer controles para los procesos y sistemas OT de la cadena de producción, incluyendo las plataformas de Planificación de Recursos Empresariales (ERP), del Sistema de Gestión Empresarial (EMS) y otros elementos como, por mencionar algunos, los sistemas de Control, Supervisor y Adquisición de Datos (Supervisory Control And Data Acquisition); los Controladores Lógicos Programables (Programmable Logical Controls) y la interfaz hombre-máquina, entre muchos otros. Una vez cubierta la protección de los sistemas OT, podrá considerarse completa la ciberdefensa de la cadena de producción crítica sectorial. Debe tenerse en mente que esta labor investigativa futura es necesaria para redondear y completar el esfuerzo efectuado en el presente trabajo.

Así pues, importante acotar que, este trabajo futuro es indispensable para completar el presente esfuerzo investigativo y que, trabajos futuros que hayan de desarrollar formalmente y en detalle, la parte de las tecnologías OT, son necesarios para completar un modelo de ciberseguridad integral para la cadena de producción crítica de la industria flexográfica, sumando a la protección aquí propuesta para la infraestructura y los sistemas de TI.

- **Evaluación del nivel de madurez en ciberseguridad de las PYMEs del sector flexográfico bajo los referentes NIST 2.0 CSF e ISO 27000 series.**

Al efecto, otra línea de investigación futura consiste en el análisis longitudinal del nivel de madurez en ciberseguridad de las PYMEs del sector flexográfico, evaluando la progresión en la implementación de controles técnicos y administrativos a partir de la adopción parcial o total del modelo de ciberseguridad basado en el CCCI propuesto en esta tesis de maestría. Esta línea podría fundamentarse en el modelo de madurez del marco NIST 2.0 CSF o en otras diversas metodologías o, permitiendo establecer correlaciones entre el nivel de madurez alcanzado y variables como el tamaño de la empresa, el grado de automatización de sus procesos, la capacitación del personal o la existencia de una política de seguridad formalizada. El objetivo sería generar una cartografía de riesgos y capacidades del sector, útil para priorizar intervenciones públicas o diseñar programas de fomento sectorial.

- **Diseño de indicadores de desempeño en ciberseguridad para la infraestructura IT de la industria flexográfica basados en buenas prácticas internacionales.**

Complementariamente, una segunda línea de investigación relevante radica en el desarrollo y evaluación de indicadores específicos de desempeño en ciberseguridad industrial, orientados al entorno particular de la industria flexográfica. Aunque existen métricas genéricas propuestas por la familia de normas ISO 27000 series (en particular por medio de la ISO 27004 a fin de establecer métricas para un SGSI) o por el propio marco NIST 2.0 CSF, el diseño de un conjunto de indicadores adaptado a las características de las empresas del sector flexográfico permitiría medir con mayor precisión la efectividad del modelo de ciberseguridad basado en el nuevo marco CCCI y en los estándares internacionales y las buenas prácticas de seguridad informática.

- **Análisis comparativo de modelos de ciberseguridad aplicados a cadenas productivas industriales: caso del sector flexográfico vs. otros sectores.**

Una tercera propuesta de investigación deriva del análisis comparativo de modelos de ciberseguridad aplicados a otros tipos de industrias y sectores que cuenten con

cadena productivas críticas, como, por ejemplo, la industria farmacéutica, alimentaria, entre otras, contrastándolos con el modelo de ciberseguridad basado en el nuevo marco CCCI y en los estándares internacionales y las buenas prácticas de seguridad informática, en esta tesis de maestría desarrollado y aplicado a la industria flexográfica. Este ejercicio permitiría identificar puntos de convergencia, divergencia y complementariedad, y establecer un marco de referencia más amplio sobre cómo se adapta la ciberseguridad a diferentes realidades productivas y a diversos entornos industriales.

Asimismo, podría servir para derivar un metamodelo de ciberseguridad industrial con componentes configurables según el tipo de industria, su criticidad, grado de automatización, exposición digital y dependencia de terceros, entre otras características importantes.

- **Modelado del impacto económico de ciberincidentes en la industria flexográfica bajo el enfoque cuantitativo del riesgo informático.**

Otra idea interesante para un quinto tema de alta proyección consiste en la evaluación del impacto económico y reputacional de los incidentes de ciberseguridad en la industria flexográfica, con el objetivo de generar modelos de cuantificación de riesgos específicos del sector. Esta línea permitiría justificar ante la alta dirección y el nivel gerencial de las empresas, la pertinencia y necesidad de inversión en ciberseguridad, traduciendo las amenazas informáticas en variables comprensibles para la toma de decisiones empresariales informadas. En este sentido, sería posible construir matrices de riesgo financiero, modelos de pérdida esperada, y escenarios de análisis costo-beneficio asociados a la implementación del modelo de seguridad basado en estándares internacionales.

- **Aplicación de inteligencia artificial para la detección proactiva de amenazas en entornos IT del sector flexográfico.**

De otra parte, una interesante sexta línea de trabajo futuro sería desarrollar un sistema basado en algoritmos de aprendizaje automático (machine learning) o aprendizaje profundo (deep learning) para la detección temprana de patrones anómalos o

actividades sospechosas en las redes informáticas asociadas a la gestión, control y operación de la cadena productiva del sector flexográfico. El modelo puede entrenarse con registros históricos de tráfico, logs de autenticación, eventos de red, e incluso indicadores propios del sistema ERP utilizado por empresas del sector flexográfico. El objetivo sería generar un sistema de detección inteligente que actúe como complemento del modelo de ciberseguridad basado en el CCCI, que incluyan al marco NIST 2.0 CSF como eje central y a las normas ISO 27000 series y a los CIS Controls como estándares adicionales de referencia, fortaleciendo la capa de "detección" con capacidades cognitivas adaptativas. Esta línea también permitiría explorar el uso de AI para garantizar la transparencia en la toma de decisiones automatizadas, lo cual es especialmente relevante en contextos industriales donde los gerentes y directivos necesitan comprender el origen y justificación de las alertas de seguridad informática.

Bibliografía y referencias

- [1] M. Dini y G. Stumpo. "MIPYMES en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento". Ed. Naciones Unidas. Proyecto "Mejores políticas para las micro, pequeñas y medianas empresas en América Latina (*EURO MIPYME*)" de la Unión Europea. Documentos de Proyectos (*LC/TS.2018/75/ Rev.1*); ISBN: 978-92-1-121987-6 (*versión impresa*) ISBN: 978-92-1-058625-2 (*versión PDF*) ISBN: 978-92-1-358092-9 (*versión ePub*). (Coordinadores - Comisión Económica para América Latina y el Caribe - CEPAL y *EURO MIPYME*). Santiago de Chile, Chile. 2020. Pág. 13. Disponible en: <https://repositorio.cepal.org/server/api/core/bitstreams/2c7fec3c-c404-496b-a0da-e6a14b1cee48/content>
- [2] F. F. Bautista Chimarro, A. E. Flores Ruiz y R. G. Aguirre Inga. "Ciberseguridad en PYMES: Caso de estudio en Cayambe". *Paper*. Revista Científica Dominio de las Ciencias. ISSN: 2477-8818 Vol. 9, núm. 4. octubre - diciembre de 2023, pp. 388-402. Disponible en: <https://dominiodelasciencias.com/ojs/index.php/es/article/view/3597>
- [3] International Standard Organization - ISO. "Norma ISO/IEC 27001:2022". 2022. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/08/84/88435.html>
- [4] Instituto Nacional de Estándares y Tecnología (NIST). "NIST 2.0 Cybersecurity Framework". Paper online. U.S. Department of Commerce. NIST CSWP -29. 26 de Febrero de 2024. Págs. 32. Disponible en: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [5] M. C. Dávila Fernández y J. Muñoz Huaman. "Diseño de controles de ciberseguridad para reducir los ciberataques en empresas distribuidoras de productos digitales basados en CIS control V8". Tesis de Pregrado. Universidad Nacional de Colombia. Facultad Nacional de Minas. Sede Medellín. Medellín. 1997. pp. 15. Disponible en: <https://repositorioacademico.upc.edu.pe/handle/10757/670133>
- [6] E. A. Acevedoarango. "Sistemas de Control Digital en Subestaciones de Alta y Extra Alta Tensión". Tesis de Pregrado. Ingeniería Eléctrica. Universidad Nacional de Colombia. Sede Medellín. Facultad Nacional de Minas. Medellín, Antioquia, Colombia. diciembre de 1996. Disponible en: *Ejemplar Físico no digitalizado*
- [7] WestRock Company, "WestRock concludes investigation into ransomware incident," *WestRock Newsroom*, 2021. [En línea]. Disponible en: <https://ir.westrock.com/press-releases/>
- [8] Label & Narrow Web, "Multi-Color Corporation addresses cyber security incident," *L&NW News*, oct. 2022. [En línea]. Disponible en: https://www.labelandnarrowweb.com/contents/view_breaking-news/2022-10-25/multi-color-corporation-addresses-cyber-security-incident/

- [9] G. Wolford, "Cybersecurity: A growing threat in the label and packaging industry," *Label & Narrow Web (LNW)*, 2025. [En línea]. Disponible en: https://www.labelandnarrowweb.com/contents/view_online-exclusives/2025-01-15/cybersecurity-a-growing-threat-in-the-label-and-packaging-industry/
- [10] E. M. Mejía Cortez. "El mercado de la flexografía en Latinoamérica". Artículo *Online*. Revista Coyuntura Económica. Instituto de Investigaciones Económicas. San Salvador. El Salvador. 16 de abril de 2024. Disponible en: <https://revistas.ues.edu.sv/index.php/coyunec/article/download/423/355>
- [11] F. Castiblanco y L. A. Oviedo Regueros. "Análisis de riesgos informáticos y sugerencia de controles para la mitigación del riesgo empleando las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 sobre los activos críticos de T.I. en la sede administrativa de la empresa Modanova S.A.S.". TGE. Trabajo de Grado. Especialización en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Bogotá, Colombia. 2017. Págs. 9. Disponible en: <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2660/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y>
- [12] H. Valencia Valencia y F. H. Orjuela Gómez, "Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa". Tesis de Grado de Maestría. Maestría en Seguridad Informática. Facultad de Ingeniería. Instituto Tecnológico Metropolitano - ITM, Medellín, 2021. Disponible en: <https://repositorio.itm.edu.co/handle/20.500.12622/5197>
- [13] Y. Z. Giraldo Montes. "Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad". Tesis de Grado de Maestría. Maestría en Seguridad Informática, Instituto Tecnológico Metropolitano - ITM, Medellín, 2020. Disponible en: <https://repositorio.itm.edu.co/handle/20.500.12622/5550>
- [14] G. B. Acuña y V. Díaz Blanco. "Mejora de Procesos de la Ciberseguridad Aeronáutica mediante un Marco de Trabajo de Madurez". Paper. Revista Cubana de Ciencias Informáticas. Vol. 17, Nro. Especial. UCIENCIA II, ISSN: 2227-1899; RNPS: 2301. Editorial "Ediciones Futuro". Universidad de las Ciencias Informáticas. La Habana, Cuba. Septiembre, 2023. Págs. 230-250. Disponible en: <https://rcci.uci.cu/index.php/RCCL/article/view/2855/865>
- [15] J. F. Hurtado Rivera, "Curso de introducción a la ciberseguridad,". Material Formativo. Asignatura Obligatoria del Núcleo Formacional de Postgrado. Campus Virtual ITM. Notas de Clase. (Semestre 01-2024), Especialización en Ciberseguridad. Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2024. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [16] S. A. Álvarez Gaviria, "Curso de Redes y Ciberseguridad". Material Formativo. Asignatura Obligatoria del Núcleo Formacional de Diplomado. Campus Virtual Universidad de Antioquia. Notas de Clase (Semestre 02-2023), Diplomado en Redes y

Ciberseguridad. Universidad de Antioquia. Convenio Sapiencia - Alcaldía de Medellín, Medellín, Colombia. 2023. Disponible en: <https://ingenia.udea.edu.co/>

- [17] **Serviflex Arco Internacional S.A.S.** "Seminario Nacional de Flexografía y Conversión Andinapack 2013. Memorias" Conferencia sobre Flexografía y Conversión. Departamento Técnico y Comercial. Ing. Edgar Alberto Acevedoarango e Ing. Adriana María Echeverri Londoño. Corferias, Auditorio Stand 11. Bogotá D.C., Colombia. 2013. Disponible en: www.serviflexarco.com
- [18] L. **Marín R.**, "Curso de Análisis y Gestión de Riesgos". Material Formativo. Asignatura Obligatoria del Núcleo Formacional de Postgrado. Campus Virtual ITM. Notas de Clase (Semestre 01-2024), Especialización en Ciberseguridad. Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2024. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [19] J. **Gil Herrera**, "Curso de Gestión de Vulnerabilidades en Aplicaciones". Material Formativo. Asignatura Obligatoria del Núcleo Formacional de Postgrado. Campus Virtual ITM. Notas de Clase (Semestre 01-2024), Especialización en Ciberseguridad. Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2024. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [20] **International Standard Organization - ISO**, "Norma ISO/IEC 27002:2022". 2022. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/07/56/75652.html>
- [21] **International Standard Organization - ISO**, "Norma ISO/IEC 27005:2022". 2022. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/08/05/80585.html>
- [22] **International Standard Organization - ISO**. "Norma ISO/IEC 31000:2018". 2022. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/06/56/65694.html>
- [23] E. A. **Acevedoarango y A. M. Echeverri Londoño**. "ICTBC (CCCI): Engineering innovation process applied in the design of an industrial cybersecurity model by improving the McCumber cube". Paper Online. Revista Universidad Militar Nueva Granada. Simposio Nacional de Maestrías y Doctorados 2025. 19avo Congreso Colombiano de Computación. Sociedad Colombiana de Computación. SCO2. 10 de noviembre de 2025. Cajicá, Cundinamarca, Colombia. p.p. z - zz. Disponible en: <https://www.umng.edu.co>
- [24] E. A. **Acevedoarango y A. M. Echeverri Londoño**. "ICTBC (CCCI): pedagogical and didactic strategy to facilitate the understanding of an industrial cybersecurity model based on an innovation engineering process through the conceptual expansion of the "McCumber cube"". Paper online. Springer Lectures Notes in Computing Science. Springer. Vol. X. Nro. Y. XX Conferencia Latinoamericana de Tecnologías de Aprendizaje. LACLO 2025. Tecnológico de Antioquia. Medellín, 7 de noviembre de 2025. PP. z - zz. Disponible en: <https://link.springer.com/book/9789819575794>.
- [25] H. F. **Vargas Montoya.**, "Curso de Seminario IV". Material Formativo. Asignatura Obligatoria de Metodología de la Investigación del Núcleo Formacional de Postgrado. Campus Virtual ITM. Notas de Clase (Semestre 02-2025), Maestría en Seguridad

Informática Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2025. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>

- [26] A. A. **Gómez** Acosta. "Curso de Gestión de Vulnerabilidades y curso de Auditoría de Seguridad Informática". Material Formativo. Asignatura Obligatoria del Núcleo Formacional de Postgrado. Campus Virtual ITM. Notas de Clase (Semestre 02-2025), Maestría en Seguridad Informática Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2025. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [27] A. M. **Ávila** Quiceno, "Curso de sistemas de detección y prevención de intrusos". Material Formativo. Asignatura Obligatoria del Núcleo Formacional de Postgrado. Campus Virtual ITM. Notas de Clase (Semestre 02-2024), Especialización en Ciberseguridad. Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2024. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [28] F.N. **Solarte** Solarte, E.R. **Enríquez** Rosero y M. del C. **Benavides**. "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001". Revista Tecnológica - ESPOL, 28(5). 2015. Disponible en: <https://rte.espol.edu.ec/index.php/tecnologica/article/view/456>
- [29] **Fig. 1.** Tipos de ciberataques comunes a empresas y PYMEs. **El Mundo**. Compartiendoconocimiento.com. "BBVA: La ciberseguridad se vuelve indispensable para las pymes". Imagen extraída de compartiendoconocimiento.com (elmundo.es). Paper Online. 2024. Disponible en: <https://compartiendoconocimiento.elmundo.es/vivencias-empresariales/la-ciberseguridad-se-vuelve-indispensable-para-las-pymes>
- [30] J. M. **González** Varona, "Retos para la transformación digital de las PYMES: competencia organizacional para la transformación digital," Tesis Doctoral. Universidad de Valladolid, Valladolid, España, 2022. Disponible en: <https://uvadoc.uva.es/bitstream/handle/10324/47767/Tesis1874-210729.pdf?sequence=1>. DOI:10.35376/10324/47767
- [31] O. **Bustillos** Ortega, y J. **Rojas** Segura. "Protocolo Básico de Ciberseguridad para PYMES". Paper. Artículo de Revista Técnica. Revista INTER FASES. Nro. 16. ISSN 1993-4912. Diciembre de 2022. p.p. 166 – 184. Disponible en: <https://revistas.ulima.edu.pe/index.php/Interfases/article/view/6021/6043>
- [32] **Fig. 2.** Tendencias en ciberataques en sectores de infraestructura crítica en Latinoamérica en 2024. N. **Cortes** Rodríguez. "La Fiscalía y Policía, las entidades encargadas de la prevención de delitos informáticos". Media Paper. Diario La República Online. Bogotá D.C., Colombia. 2024. Disponible en: <https://www.larepublica.co/internet-economy/en-colombia-la-fiscalia-y-policia-las-encargadas-de-prevenir-los-delitos-informaticos-3802915>
- [33] S. A. **Berru** Escajadillo, y L. F. **Yarleque** Golles. "Propuesta Metodológica para mitigar los riesgos sobre ciberataques a PYMEs, usando la metodología NIST". TGP. Tesis de Pregrado. Ingeniería de Sistemas. Facultad de Ingeniería y Arquitectura. Universidad César Vallejo. Piura, Perú. 2023. Págs. 95. Disponible en:

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/128701/Berru_ESA-Yarleque_GLF-SD.pdf?sequence=1&isAllowed=y

- [34] A. **Cardona** Londoño y D. L. **Carvajal** Portilla, "Diseño del sistema de gestión de seguridad de la información basado en la familia de normas de la serie ISO/IEC 27000 para una entidad pública colombiana," TGM. Tesis de Maestría. Universidad Autónoma de Manizales. Manizales, Colombia. 2018. Disponible en: <https://repositorio.autonoma.edu.co/items/ca3a97c1-3e66-4c2a-836e-d58a65ed5f80>
- [35] **Fig. 3. Tendencias globales de ciberataques por tipo de industria en 2024. INTEREMPRESAS.NET.** "Aumentan un 28% los ciberataques a nivel mundial en el primer trimestre de 2024, según Check Point Research". Paper Online. 16 de abril de 2024. Disponible en: <https://www.interempresas.net/Ciberseguridad/Articulos/559363-Aumentan-28-por-ciento-ciberataques-nivel-mundial-primer-trimestre-2024-segun-Check-Point.html>
- [36] **Asociación Colombiana de la Industria de la Comunicación Gráfica (ANDIGRAF).** "Feria Andigráfica Bogotá D.C. 2025" Feria Industrial de las Artes Gráficas de Colombia. Corferias. Bogotá D.C., Colombia. 17 al 20 de junio de 2025. Disponible en: <https://www.andigraf.com.co/eventos-andigraf/andigrafica/>
- [37] **Instituto de Ciberseguridad de España (INCIBE).** "Cumpliendo con la NIS2: Recursos y servicios para la pyme". Artículo *Online*. INCIBE. 16 de Abril de 2024. Disponible en: <https://www.incibe.es/empresas/blog/cumpliendo-con-la-nis2-recursos-y-servicios-para-la-pyme>
- [38] E. **Fernández** García. "Derecho de la Ciberseguridad de las Infraestructuras Críticas: Más allá de la perspectiva penalista". *Paper*. Revista Jurica de Castilla y León. N. 56. ISSN: 1696-6759. Castilla, España. Enero 2022. Págs. 109–141. Disponible en: <https://portalcientifico.upsa.es/documentos/635b1ff62a69e15fc7213ca9>
- [39] G. **Peri.** "Cadenas de Producción. Análisis de Protección Efectiva. Informe Final". Paper. Fundación INAI. Buenos Aires, Argentina. Septiembre de 2009. p.p. 99. Disponible en: https://www.inai.org.ar/archivos/notas/peri_informe_final_cadenas_productivas.pdf
- [40] J. **Anabalón R.** y E. **Donders O.** "Revisión de ciberdefensa de infraestructura crítica". Paper. Revista Estudios de Seguridad y Defensa (ESD) Nro. 3, ANEPE. Junio de 2014, p.p. 131 - 164. Disponible en: https://silo.tips/queue/una-revision-de-ciberdefensa-de-infraestructura-critica?&queue_id=1&v=1725411643&u=MjgwMDo0ODQ6OTg5NDpiODAwOmE0MTY6YWE2Ojk3NWU6YmE5YQ==
- [41] H.R. **Colombo**, J. **Kamlosfsky**, J. M. **Pedernera** Gaitán y M. N. **Sliafertis**. "Un enfoque para disminuir los efectos de los Ciber-ataques a las Infraestructuras Críticas". Paper Online. Sistema Pedagógico Vaneduc (SPV). Referenciado de Researchgate.net. Noviembre de 2015. Disponible de pago en: <https://imgbiblio.vaneduc.edu.ar/fulltext/files/TC121046.pdf>
- [42] J. **Quintana**, F. **Cornejo** y A. **Rigail** Cedeño. "Análisis y diseño de empaques flexibles para alimentos". *Paper*. Revista Tecnológica ESPOL, Vol. 20, N. 1, 11-18, ISSN: 0257-1749. Guayaquil, Guayas, Ecuador. Agosto - octubre, 2007. Disponible en: <https://rte.espol.edu.ec/index.php/tecnologica/article/view/156/100>

- [43] M. D. **Vidales** Giovannetti. "Antología Flexográfica". Ed. Universidad Autónoma Metropolitana. Libro. División de Ciencias y Artes para el Diseño. ISBN: No tiene. México. 1996. p.p 94. Disponible en: <https://files.core.ac.uk/download/48393491.pdf>
- [44] **Fig. 4.** Web site corporativo de una empresa del sector flexográfico. Serviflex Arco Internacional S.A.S. Imagen de autoría propia. 2024. Disponible en: www.serviflexarco.com y www.cleanlox.com
- [45] J. **García** Anduiza. "Gestión de la cadena de suministro: análisis del uso de las TIC y su impacto en la eficiencia". Tesis Doctoral. Universidad Complutense de Madrid. Facultad de Ciencias Económicas y Empresariales. Madrid, España. 2018. p.p. 215. Disponible en: <https://docta.ucm.es/rest/api/core/bitstreams/219d2d22-be04-493b-b815-eeb4d27a49f9/content>
- [46] **Fig. 5.** Prevención en Seguridad Informática: Analogía con la infraestructura esencial del sector Salud. **culturapreventivaosarten.com**. "Las necesidades y la cultura preventiva". Imagen extraída de Culturapreventivaosarten.com. 2024. Disponible en: <https://culturapreventivaosarten.com/necesidad-seguridad/>
- [47] **Fig. 6.** Infraestructura de producción de una empresa esencial del sector flexográfico. **envapack.com**. "Planta de Establecimiento Gráfico con Cadena de Producción de última generación (Bobst)". Imagen extraída de envapack.com. 2024. Disponible en: <https://www.envapack.com/2019/05/establecimiento-grafico-impresores-continua-creciendo-en-el-mercado-de-embalaje-flexible-con-impresoras-flexo-de-tambor-central-y-maquinas-laminadoras-bobst/>
- [48] H. **Valencia** Valencia y F. H. **Orjuela** Gómez. "Curso de Plan de Continuidad del Negocio y Gestión de Crisis ". Material Formativo. Asignatura Optativa de Profundización. Campus Virtual ITM. Notas de Clase (Semestre 01-2024), Especialización en Ciberseguridad. Instituto Tecnológico Metropolitano - ITM, Medellín, Colombia. 2024. Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [49] E. A. **Acevedoarango** y A. M. **Echeverri** Londoño. "Del cubo Rubik a la ciberseguridad industrial". Paper Online. Revista Institucional La Tekné. ed. 116 No. 2025-2. Fondo Editorial ITM. Institución Universitaria ITM. Medellín. Colombia. 14 de Octubre de 2025. Pp. 10 - 16. Disponible en: <https://catalogo.itm.edu.co/gpd-la-tekhne-n-116--68ee8fb056f25.html>.
- [50] **International Standard Organization - ISO**. "Norma ISO 22301:2019" 2019. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/07/51/75106.html>
- [51] **International Standard Organization - ISO**. "Norma ISO 22361:2022". 2022. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/05/02/50267.html>
- [52] **International Standard Organization - ISO**. "Norma ISO 22316:2017". 2017. Disponible de pago en: <https://www.iso.org/es/contents/data/standard/05/00/50053.html>
- [53] R. D. **Villa** Trujillo. "Modelo de ciberseguridad en las unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico nacional". Tesis de Maestría en Seguridad Informática. Facultad de Ingenierías. Grupo de Investigación en Automática y Electrónica y Ciencias

- computacionales. Institución Universitaria ITM. Medellín, Antioquia, Colombia. 2019. pp. 94. Disponible en: <https://repositorio.itm.edu.co/entities/publication/83f79046-ea9e-4ce6-a6ac-d6aa1c85ef41>
- [54] M. J. **Caro** Bejarano. “La protección de las infraestructuras críticas”. Paper online. Revista Documento Análisis. Instituto Español de Estudios Estratégicos (IEEE) (<https://revista.ieee.es/>). ISSN 2255-3479. Madrid, España. 27 de Julio de 2011. p.p. 7. Disponible en: <https://dialnet.unirioja.es/servlet/articulo?codigo=7429659>
- [55] B. **Orantos**. “Plan director de seguridad de una infraestructura crítica”. Universitat Politècnica de València. 2022. Disponible en: <http://hdl.handle.net/10251/186006>
- [56] K. **Kraugusteeliana**, S. S. **Wahyuningsih**, I H. **Indriana**, D, **Suryadi**, y M. **Munizu**. “The Application of COBIT Framework to Evaluate Information System Governance in National Business Technology Transformation Companies”. Jurnal Informasi dan Teknologi. Vol. 6 No. 1; e-ISSN: 2714-9730; Page: 86-92; 2024. Disponible en: <https://pdfs.semanticscholar.org/19b5/24be54089b58ba4c308065878438df7a3e04.pdf>
- [57] C. R. **Hernández** Sampieri, C. **Fernández** Collado y P. **Baptista** Lucio. “Metodología de la investigación”. 6ta ed. Ed. MacGraw-Hill. ISBN: 978-1-4562-2396-0. México, México. 2014. Disponible en: https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf
- [58] J. **Casas** Anguita, J. R. **Repullo** Labrador y J. **Donado** Campos. “La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I)”. Paper Online. Revista Atención Primaria. Ed. SemFYC. Volumen 31, Issue 8, 2003, Págs. 592 – 600 (92-108). Disponible en: <https://pmc.ncbi.nlm.nih.gov/articles/PMC7681832/>
- [59] J.R. **McCumber**. “Information Systems Security: A Comprehensive Model.” Paper Online [En Línea] (Original Paper). National Institute of Standards and Technology (NIST) / National Computer Security Center (NCSC). “14th National Computer Security Conference”. Memories. Paper referred. NIST/NCSC. Omni Shoreham Hotel. Washington, D.C. Estados Unidos de América. 14 de octubre, 1991. Pág. 328 – 337 de 372. Disponible en: <https://csrc.nist.gov/files/pubs/conference/1991/10/01/proceedings-14th-national-computer-security-confer/final/docs/1991-14th-ncsc-proceedings-vol-1.pdf>
- [60] J. **Gámiz**. “Fundamentos clave para proteger la información (CIA), Cubo de McCumber de la seguridad informática”. Presentación tridimensional cubica”. Paper Online. www.joaquingamiz.substack.com. 24 de Julio de 2024. Disponible en: <https://joaquingamiz.substack.com/p/fundamentos-clave-para-proteger-la>
- [61] **NCYTE CENTER**. “The McCumber Cube and CIA Triad”. Paper Online. [En línea]. www.ncyte.net. National Science Foundation. DUE 1601612. Disponible en: <https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad>

Anexos

Ver los siguientes anexos en documentos PDF y Excel adjuntos al final de este informe final de tesis de maestría en seguridad informática.

Anexo Nro. 1. Diagnóstico del estado actual y necesidades de la seguridad de la información del sector flexográfico.

Anexo Nro. 2. Tabulación de resultados de encuesta de diagnóstico del estado actual y necesidades de la seguridad de la información en el sector flexográfico.

Anexo Nro. 3. Autodiagnósticos obtenidos de los resultados de la encuesta de diagnóstico sectorial flexográfico (Autoevaluaciones según norma ISO 27001 y marco NIST 2.0 CSF).

Anexo Nro. 4. Matriz de riesgo informático y mapa de calor - Análisis y evaluación del riesgo cibernético actual del sector flexográfico.

Anexo Nro. 5. Controles seleccionados de la revisión de estándares internacionales y buenas prácticas de seguridad informática para el sector flexográfico.

Anexo Nro. 6. Modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Anexo Nro. 7. Validación del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Anexo Nro. 8. Tabulación y análisis de resultados de la encuesta de validación final del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Anexo Nro. 9. Autodiagnósticos finales obtenidos de los resultados de la encuesta de verificación del modelo de ciberseguridad (Autoevaluaciones según norma ISO 27001 y marco NIST 2.0 CSF).

Anexo Nro. 10. Matriz de riesgo informático y mapa de calor finales - Análisis y evaluación del riesgo cibernético final basada en los resultados obtenidos de la prueba de concepto (encuesta de verificación) realizada para validación del modelo de ciberseguridad.

Anexo Nro. 11. Nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI) New Industrial Cybersecurity Tinker Bell Cube (ICTBC) framework

Anexo Nro. 12. Estructura metodológica de investigación que condujo a la creación del nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI).

Anexo Nro. 13. Productos de esta tesis de maestría en seguridad informática. Artículos publicados, o confirmados y a publicar, en revistas indexadas.

Anexo 14. Productos de esta tesis de maestría en seguridad informática Participaciones, cursos y eventos. Certificaciones obtenidas en eventos, cursos y capacitaciones realizados durante y para el desarrollo de esta investigación de tesis de maestría en seguridad informática.



Institución Universitaria

Medellín, 07 de abril de 2026.

ANEXOS

Anexo Nro. 1

Diagnóstico del estado actual y necesidades de la seguridad de la información del sector flexográfico

Ver archivo PDF anexo (Anexo Nro. 1 - .pdf)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 1 - Actividad 1.1 - ENTREGABLE

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño
Maestría en Seguridad Informática
I.T.M.

I.T.M.

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Ing. **Edgar Alberto Acevedoarango** e Ing. **Adriana María Echeverri Londoño**

DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR FLEXOGRÁFICO

ENCUESTA PARA TESIS DE MAESTRÍA

Sección 1 - CONSENTIMIENTO INFORMADO

Con el fin de realizar un diagnóstico que permita evaluar el estado actual y los requerimientos de seguridad de la información y ciberseguridad de la infraestructura informática asociada a la cadena productiva de las Pymes y empresas de la industria flexográfica, le solicitamos su amable y apreciada participación en esta encuesta, que pretende dar solución, a una necesidad sentida del sector, respecto a la seguridad informática de la infraestructura, los sistemas y equipos computacionales asociados a la gestión y operación de la línea de producción del sector flexográfico.

Como bien se comprende la línea de producción es una infraestructura tan crítica, como neurálgica, para el adecuado y normal funcionamiento de una compañía flexográfica y, por tal razón, se trata de un conjunto valioso e irremplazable de activos muy sensibles, esenciales e insustituibles que, a través de la infraestructura, sistemas y equipos informáticos, usados para su acceso, manejo y control, pueden ser altamente susceptibles al riesgo de ocurrencia de un incidente de ciberseguridad que, afecte, interrumpa o colapse, la cadena de producción y, por ende, que impacte sobre toda la compañía en general. Los incidentes de seguridad informática y ciberseguridad son eventos que, aprovechando vulnerabilidades o brechas de seguridad, atacan las líneas y los procesos productivos sensibles de la operación industrial, por medio de afectaciones a la infraestructura, el sistema y los equipos computacionales que gestionan y operan dichas cadenas de producción y, que tienen la capacidad de impactar, interrumpir, colapsar, e incluso, de llegar a dañar o destruir, parcial o totalmente, un equipo o máquina, o un conjunto de ellos, perturbando la operación de las compañías y, eventualmente, llegando a interrumpir su funcionamiento durante un largo periodo de tiempo o paralizarlo totalmente.

Así pues, en razón a que el control y operación de la cadena de producción, en la actualidad, se realiza a través de un sistema o dispositivo informático que, adicionalmente, también, puede estar

permanente, o parcialmente, conectado a una red o conjunto de redes, ya locales (con otras áreas de la empresa, calidad, ventas, comercial, compras, etc.) o ya externas, como el internet, para diversos efectos (mantenimiento, seguimiento, supervisión, ajuste fino, cambio de configuración o de parámetros de operación, etc.) mediante conexión remota con la casa fabricante, es importante proteger dicha infraestructura y garantizar su continuidad y resiliencia operativas.

Los ciberataques son un cierto tipo de incidentes informáticos maliciosos que, pueden llegar a impactar gravemente a una compañía y, en particular, a su línea productiva. De otra parte, las empresas y, en especial, sus sistemas informáticos asociados a sus cadenas de producción, también, pueden ser susceptibles a la ocurrencia de contingencias, fallas tecnológicas, calamidades o desastres, eventos, todos, para los cuales, las compañías, también, deben prepararse con la debida antelación y, sobre todo, saber cómo enfrentar, responder y superar.

En este sentido, su colaboración es valiosa, importante y completamente voluntaria y, para su total tranquilidad, sus respuestas serán tratadas de manera confidencial, solo y exclusivamente para efectos de realizar un diagnóstico sectorial que permita consolidar la evaluación y el análisis del riesgo informático en las PYMES y empresas de la industria flexográfica y solo será utilizada exclusivamente para fines académicos y de investigación en la elaboración de una tesis de Maestría en Seguridad Informática.

Es importante hacer notar que la información proporcionada en esta encuesta será manejada con estricta ética, legalidad y confidencialidad, conforme a lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, que regulan la protección de datos personales y tratamiento de información sensible en Colombia. Los datos recabados serán utilizados exclusivamente para los fines de estudio académico e investigativo manifestados y no serán compartidos con terceros ajenos a la investigación realizada. Asimismo, se garantizará que, todos los datos sean almacenados de manera segura y se adoptarán las medidas necesarias para evitar su acceso no autorizado por parte de terceros no autorizados. En todo momento, durante el desarrollo y consolidación de los datos de esta encuesta, usted y su institución, o compañía, tendrán derecho a consultar, actualizar, rectificar o suprimir sus datos personales o información sensible, así como a revocar la autorización suministrada para su tratamiento y uso, conforme a los procedimientos establecidos en la legislación colombiana.

Si está de acuerdo en participar y responder a esta encuesta, por favor marque "Sí"; de lo contrario, marque "No".

Si ____ No ____

Sección 2 – ESCALA DE LIKERT PARA OPCIONES DE RESPUESTA

ESCALA DE LIKERT PARA VALORACIÓN DE RESPUESTAS DE LA ENCUESTA				
Escala de Valores		Respuestas posibles		
Letras	Números			
Cero	0	No tiene implementación de Ciberseguridad alguna.	Ninguna	Totalmente en desacuerdo
Uno	1	Tiene solamente una implementación de Ciberseguridad incipiente	Poca	En desacuerdo
Dos	2	Tiene una algún tipo de implementación muy básica de Ciberseguridad que no logra brindar protección completa	Regular	Neutral
Tres	3	Tiene una algún tipo de implementación funcional de Ciberseguridad que brinda un muy moderado nivel de seguridad.	Mucha	De acuerdo
Cuatro	4	Tiene una implementación de Ciberseguridad buena y suficiente.	Casi toda	Muy de acuerdo
Cinco	5	Tiene una implementación de Ciberseguridad completa y total basada en normas y estándares internacionales	Toda	Totalmente de acuerdo

Nota: El valor Cero (0) expresa: no hay, no se tiene, no se realiza, no se está de acuerdo, no ha pasado, mientras que Cinco (5) expresa el extremo contrario, i.e., si hay, si se tiene, si se realiza, si se está completamente de acuerdo; mientras que los valores intermedios expresan la moderación entre ambos extremos según el contexto de la pregunta.

Contactos:

info3@serviflexarco.com / sales2@serviflexarco.com

Para más información, dudas o inquietudes, los participantes pueden contactar a:

- Ing. **Edgar Alberto Acevedoarango:**
317 452 23 26 - edgaracevedoarango1131337@correo.itm.edu.co
- Ing. **Adriana María Echeverri Londoño.**
317 510 38 60 - adrianaecheverri1131341@correo.itm.edu.co

Sección 3 - ENCUESTA

Por favor, marque con una Equis (X) la respuesta que considere pertinente y un fiel reflejo de la situación de ciberseguridad en su empresa.

1. ¿Su empresa cuenta con una estrategia, plan o protocolo de ciberseguridad o de manejo de incidentes cibernéticos, formalmente implementado, que asegure la confiabilidad, integridad y disponibilidad de sus sistemas y equipos informáticos, en especial los de su cadena de producción?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

2. ¿Su empresa tiene formalmente implementadas medidas de seguridad, como antivirus o antimalware licenciados, para proteger los sistemas informáticos y la información corporativa contra amenazas maliciosas, como ataques cibernéticos?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

3. ¿Su empresa cuenta con personal o un departamento de ciberseguridad que asegure la confiabilidad, integridad y disponibilidad de su infraestructura y equipos informáticos, en especial los de su cadena de producción?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

4. ¿Existen controles, como contraseñas seguras con factor de doble autenticación (2FA), en los equipos informáticos de gestión y operación de la producción que restringen el acceso a personal no autorizado?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

5. ¿Los empleados, incluido el personal de planta y de producción, reciben capacitación regular y periódica sobre buenas prácticas de seguridad informática?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

6. ¿La empresa tiene un sistema de respaldo (copias de seguridad o Backups), ya sea físico o en la nube, de su información crítica, en especial la de su cadena de producción?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

7. ¿La empresa evalúa y analiza de manera formal, regular y periódica, el nivel de riesgo cibernético asociado con la seguridad informática de sus equipos, sistemas y dispositivos informáticos, en especial de aquellos que están asociados a la gestión y operación de los procesos de producción?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

8. ¿Existe en su empresa un compromiso directivo y de la alta gerencia con respecto a la seguridad informática y la ciberseguridad de la organización?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

9. ¿Su empresa cuenta con maquinaria o equipos de su línea de producción que tengan conexión eventual, temporal o permanente a internet o a otras redes, ya sean internas (LAN – Red corporativa, como la del área de calidad, mantenimiento, etc.) o externas (proveedores, fabricantes, clientes, etc.)?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

10. ¿Ha sufrido su empresa incidentes o ataques informáticos en el pasado?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

11. Utiliza un equipo computacional viejo y obsoleto en su cadena de producción?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

12. ¿Qué sistema operativo utiliza(n) su(s) equipo(s) computacional(es) asociados a la gestión de su cadena de producción?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

Win XP ____ Win 7 ____ Win 8 ____ Win10 ____ Win11 ____
Linux ____ MacOS ____ Otro ____ Cuál? _____

Anexo Nro. 2

Tabulación de resultados de encuesta de diagnóstico del estado actual y necesidades de la seguridad de la información en el sector flexográfico

Ver archivos Excel (Anexo Nro. 2 - .xlsx)

En este anexo, también, se consigna el análisis efectuado de los resultados obtenidos y los autodiagnósticos consolidados (según norma ISO 27001 y marco NIST 2.0 CSF)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 1 - Actividad 1.1 – ENTREGABLE

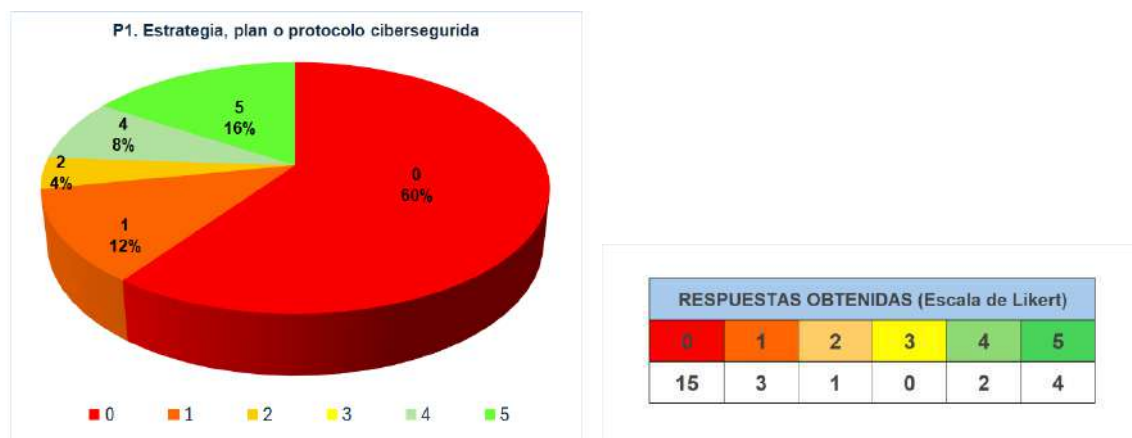
Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño
Maestría en Seguridad Informática
I.T.M.

Tabulación de resultados de encuesta de diagnóstico del estado actual y necesidades de la seguridad de la información en el sector flexográfico

Resultados obtenidos y análisis estadístico de la encuesta de “Diagnóstico del estado actual y necesidades de la seguridad de la información del sector flexográfico”

A continuación, se consignan los resultados obtenidos y su respectivo análisis estadístico y conceptual. También, se consignan las autoevaluaciones derivadas que servirán de insumo para la elaboración del análisis y evaluación de riesgo mediante la construcción de la matriz de riesgo y su mapa de calor.

Pregunta 1 - ¿Su empresa cuenta con una estrategia, plan o protocolo de ciberseguridad o de manejo de incidentes cibernéticos, formalmente implementado, que asegure la confiabilidad, integridad y disponibilidad de sus sistemas y equipos informáticos, en especial los de su cadena de producción?



Resultados obtenidos en la primera pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la primera pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico. Gráfico de tarta o circular y tabulación detallada. Fuente: Autoría propia.

Como se puede observar, la industria flexográfica, en su gran mayoría (76%) no cuenta con estrategias, protocolos, planes o mecanismos formales de ciberseguridad para protección de su infraestructura informática.

Como demuestran los resultados obtenidos, esta circunstancia pone en grave riesgo la confiabilidad, integridad y disponibilidad de los sistemas y equipos informáticos, en especial, de todos aquellos asociados a la gestión, control y operación de las cadenas de producción crítica y esencial de las PYMEs y empresas del sector. Consecuentemente, los resultados obtenidos corroboran la justificación, urgencia e importancia de esta tesis de maestría.

Pregunta 2 - ¿Su empresa tiene formalmente implementadas medidas de seguridad, como antivirus o antimalware licenciados, para proteger los sistemas informáticos y la información corporativa contra amenazas maliciosas, como ataques cibernéticos?

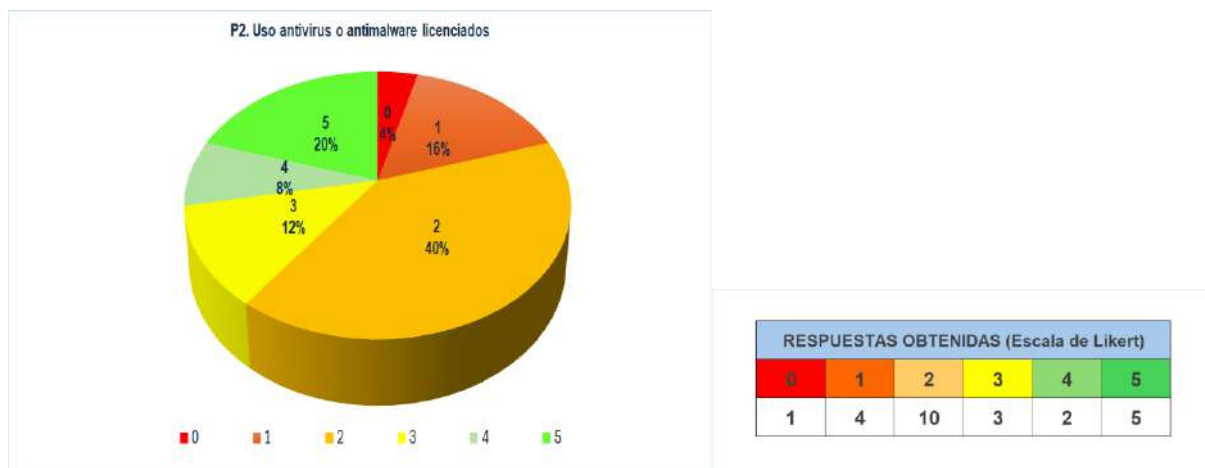


Fig. A1.2

Resultados obtenidos en la segunda pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la segunda pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Como se puede observar, la industria flexográfica, en mayoría (52%) no cuenta con antivirus o antimalware licenciados, para proteger sus sistemas informáticos y la información corporativa contra amenazas maliciosas, como ataques cibernéticos.

Como demuestran los resultados obtenidos, al igual que en el caso anterior, esta circunstancia pone en grave riesgo la confiabilidad, integridad y disponibilidad de los sistemas y equipos informáticos, en especial, de todos aquellos asociados a la gestión, control y operación de las cadenas de producción crítica y esencial de las PYMEs y empresas del sector. Consecuentemente, los resultados obtenidos corroboran la justificación, urgencia e importancia de esta tesis de maestría.

Pregunta 3 - ¿Su empresa cuenta con personal o un departamento de ciberseguridad que asegure la confiabilidad, integridad y disponibilidad de su infraestructura y equipos informáticos, en especial los de su cadena de producción?

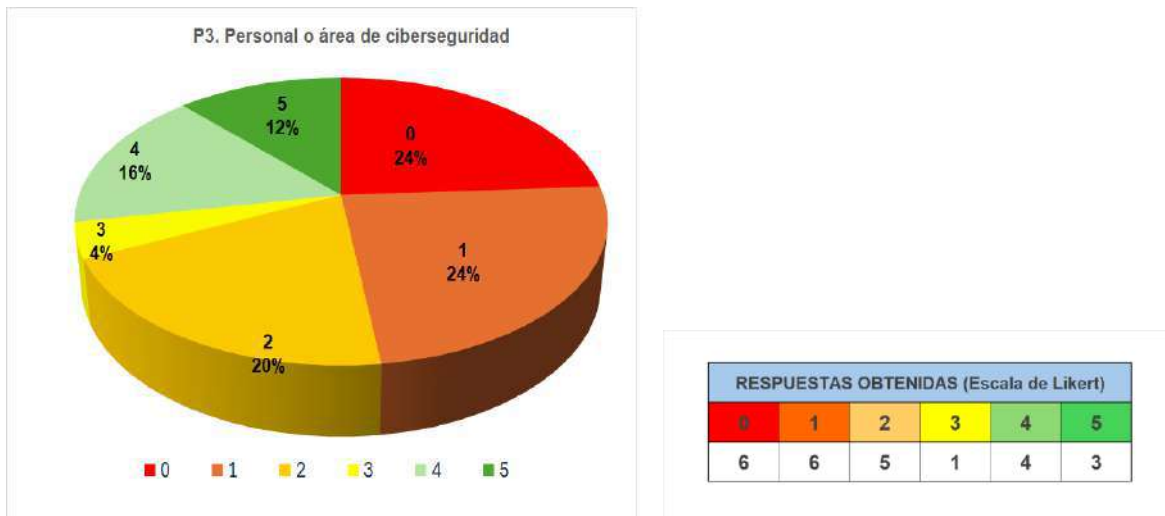


Fig. A1.3

Resultados obtenidos en la tercera pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la tercera pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Como se puede observar, la industria flexográfica, en su gran mayoría (72%) no cuenta con personal calificado y experto o con un departamento de ciberseguridad formalmente implementado, para proteger sus sistemas informáticos y la información corporativa contra ciberataques o incidentes.

Como demuestran los resultados obtenidos, al igual que en los casos anteriores, esta circunstancia pone en grave riesgo la confiabilidad, integridad y disponibilidad de los

sistemas y equipos informáticos, en especial, de todos aquellos asociados a la gestión, control y operación de las cadenas de producción crítica y esencial de las PYMEs y empresas del sector. Consecuentemente, los resultados obtenidos corroboran la justificación, urgencia e importancia de esta tesis de maestría.

Pregunta 4 - ¿Existen controles, como contraseñas seguras con factor de doble autenticación (2FA), en los equipos informáticos de gestión y operación de la producción que restringen el acceso a personal no autorizado?

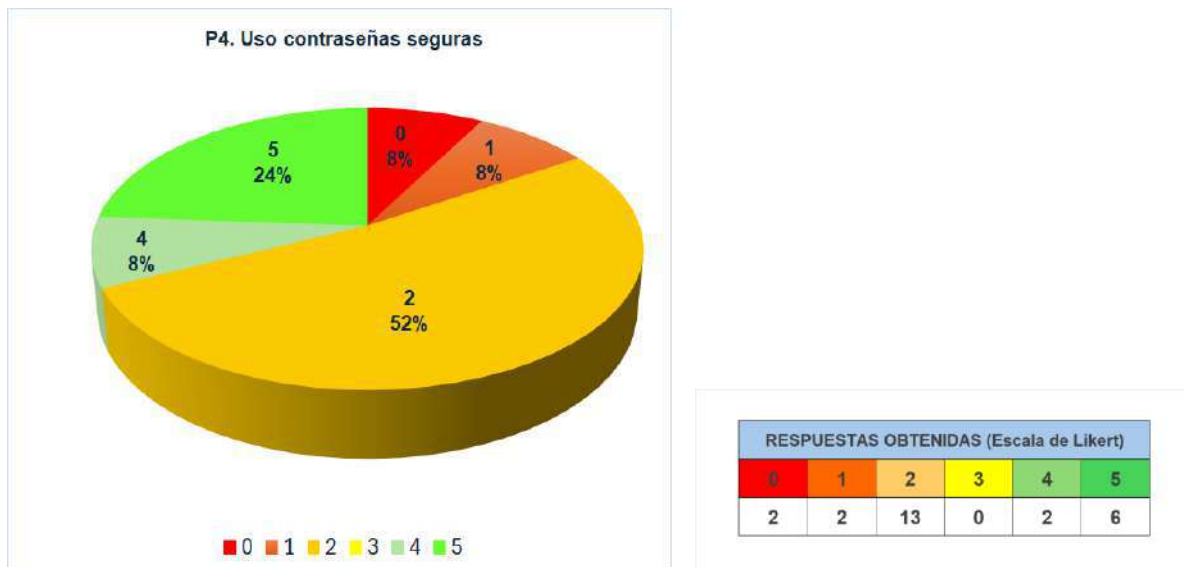


Fig. A1.4

Resultados obtenidos en la cuarta pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la cuarta pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Como se puede observar, la industria flexográfica, en su gran mayoría (72%) no cuenta con personal calificado y experto o con un departamento de ciberseguridad formalmente implementado, para proteger sus sistemas informáticos y la información corporativa contra ciberataques o incidentes.

Como demuestran los resultados obtenidos, al igual que en los casos anteriores, esta circunstancia pone en grave riesgo la confiabilidad, integridad y disponibilidad de los sistemas y equipos informáticos, en especial, de todos aquellos asociados a la gestión, control y operación de las cadenas de producción crítica y esencial de las PYMEs y

empresas del sector. Consecuentemente, los resultados obtenidos corroboran la justificación, urgencia e importancia de esta tesis de maestría.

En razón a que los análisis de las siguientes preguntas son análogos a los anteriormente efectuados, se omitirán por brevedad.

Pregunta 5 - ¿Los empleados, incluido el personal de planta y de producción, reciben capacitación regular y periódica sobre buenas prácticas de seguridad informática?

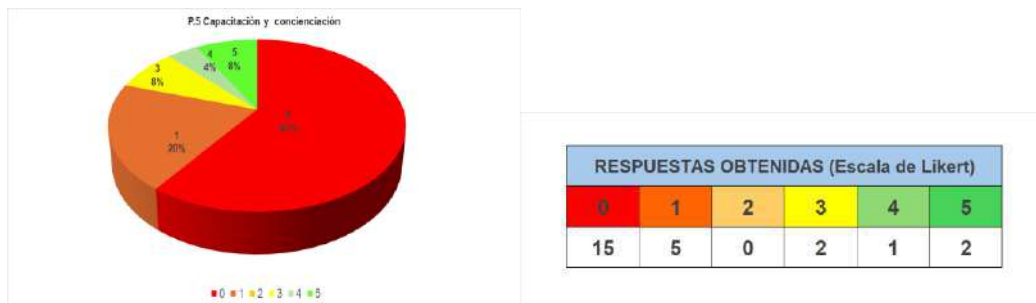


Fig. A1.5

Resultados obtenidos en la quinta pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la quinta pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Pregunta 6 - ¿La empresa tiene un sistema de respaldo (copias de seguridad o backups), ya sea físico o en la nube, de su información crítica, en especial la de su cadena de producción?



Fig. A1.6

Resultados obtenidos en la sexta pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la sexta pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Pregunta 7 - ¿La empresa evalúa y analiza de manera formal, regular y periódica, el nivel de riesgo cibernético asociado con la seguridad informática de sus equipos, sistemas y dispositivos informáticos, en especial de aquellos que están asociados a la gestión y operación de los procesos de producción?

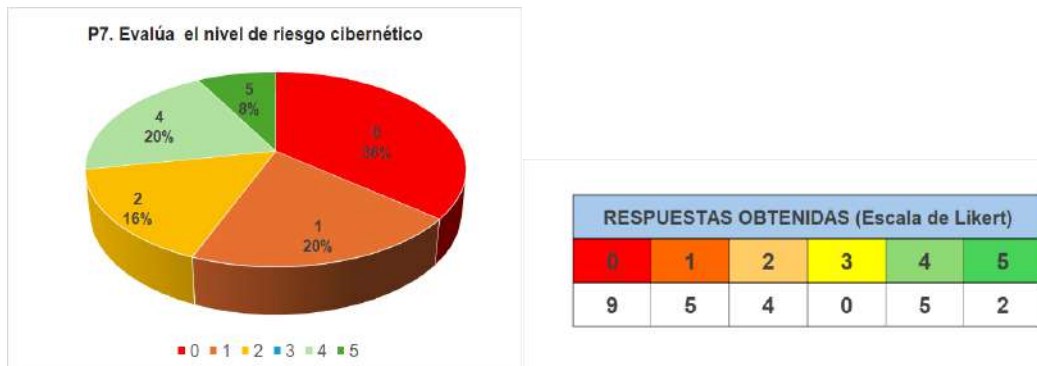


Fig. A1.7

Resultados obtenidos en la séptima pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la séptima pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Pregunta 8 - ¿Su empresa cuenta con maquinaria o equipos de su línea de producción que tengan conexión eventual, temporal o permanente a internet o a otras redes, ya sean internas (LAN. red corporativa, como la del área de calidad, mantenimiento, etc.) o externas (proveedores, fabricantes, clientes, etc.)?

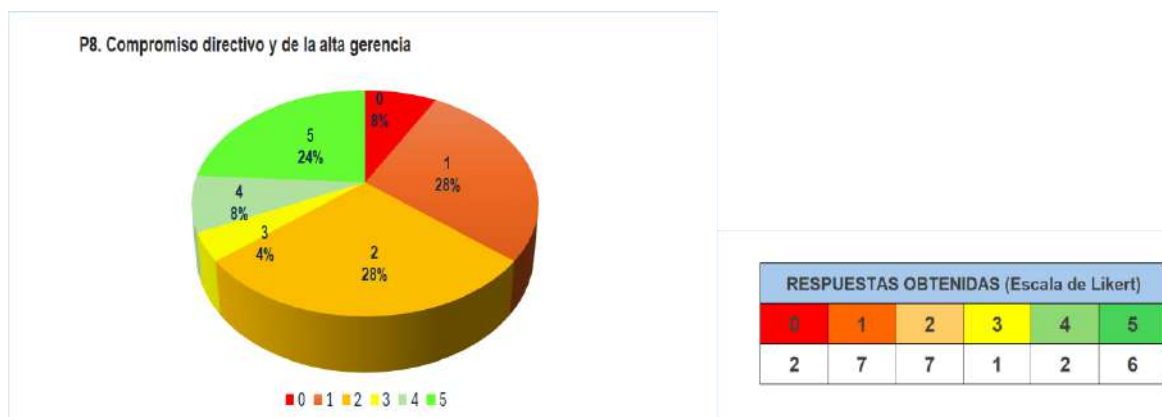


Fig. A1.8

Resultados obtenidos en la octava pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la octava pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Pregunta 9 - ¿Su empresa cuenta con maquinaria o equipos de su línea de producción que tengan conexión eventual, temporal o permanente a internet o a otras redes, ya sean internas (LAN, red corporativa, como la del área de calidad, mantenimiento, etc.) o externas (proveedores, fabricantes, clientes, etc.)?

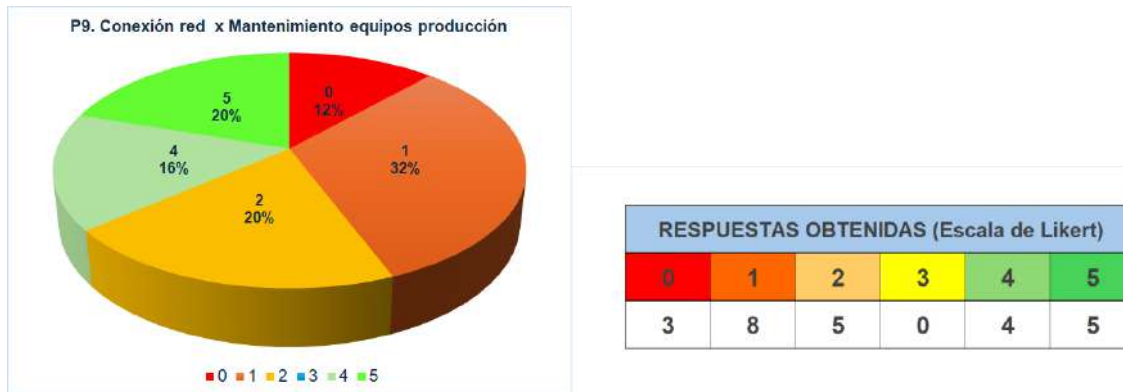


Fig. A1.9

Resultados obtenidos en la novena pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la novena pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Pregunta 10 - ¿Ha sufrido su empresa, incidentes o ataques informáticos en el pasado?

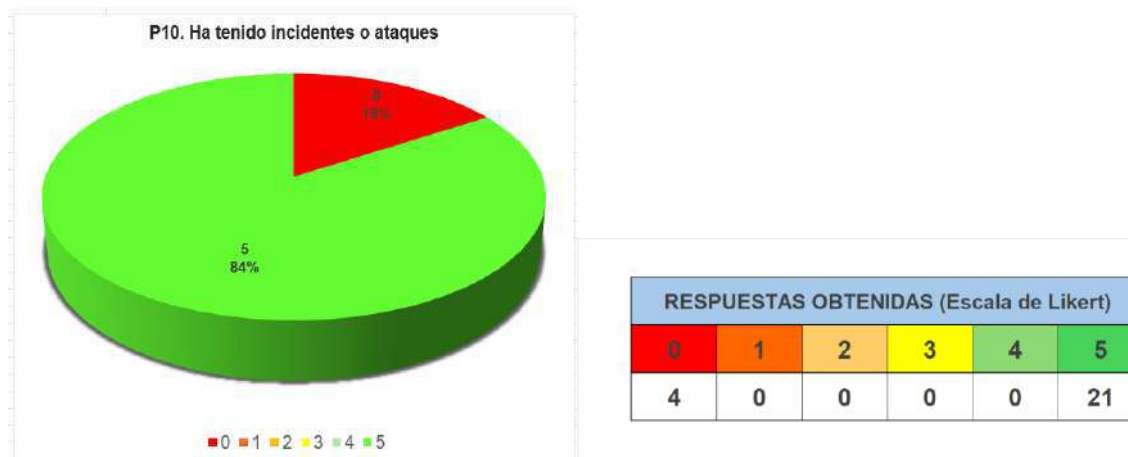


Fig. A1.10

Resultados obtenidos en la décima pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la décima pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Pregunta 11 - ¿Utiliza un equipo computacional viejo y obsoleto en su cadena de producción?

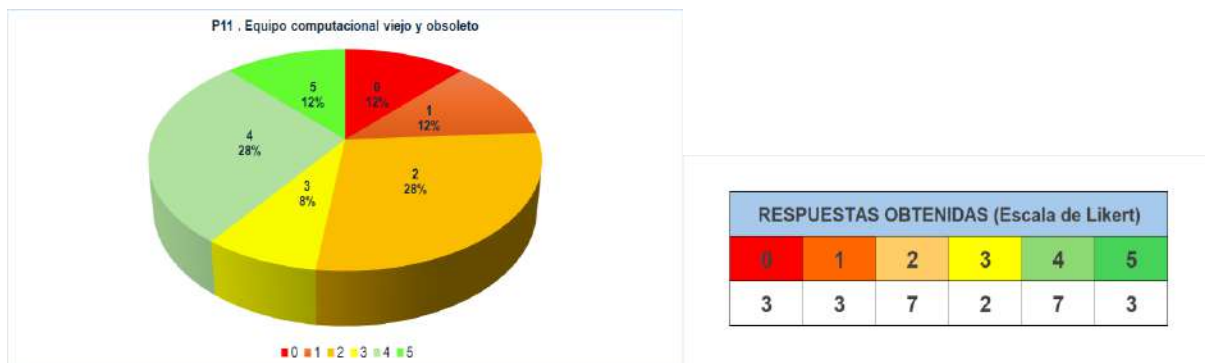


Fig. A1.11

Resultados obtenidos en la décima primera pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de torta y tabulación detallada.

Nota: Resultados obtenidos en la décima primera pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de torta y tabulación detallada. Fuente: Autoría propia.

Pregunta 12 - ¿Qué sistema operativo utiliza(n) su(s) equipo(s) computacional(es) asociados a la gestión de su cadena de producción?



Fig. A1.12

Resultados obtenidos en la décima segunda pregunta de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de torta y tabulación detallada.

Nota: Resultados obtenidos en la décima segunda pregunta de la encuesta de diagnóstico de estado y requerimientos de seguridad de la información en el sector flexográfico 2025. Gráfico de torta y tabulación detallada. Fuente: Autoría propia.

Nota Importante:

Para mayor detalle sobre los resultados obtenidas en la encuesta, por favor, ver Anexo Nro. 3 (Excel).

Con base en los anteriores resultados y, tal como formulan [56] y [57], se realizó un análisis cuantitativo y cualitativo de las respuestas obtenidas en las doce (12) preguntas formuladas mediante la aplicación del instrumento, así como, también, se identificaron los sistemas operativos utilizados en la gestión de las cadenas de producción esenciales de las PYMEs y empresas de la industria flexográfica. A continuación, se resumen los principales hallazgos, destacando fortalezas, debilidades y áreas de oportunidad para el sector flexográfico en cuanto la ciberseguridad, a saber:

Análisis conceptual de los resultados del instrumento aplicado.

A continuación, se presenta el análisis cuantitativo y cualitativo por cada pregunta de la encuesta aplicada con base en los resultados en ella obtenidos.

Como se observó anteriormente, la encuesta aplicada utilizó una escala de Likert de Cero (0) (totalmente en desacuerdo/nunca/no implementado, etc) a Cinco (5) (totalmente de acuerdo/siempre/bien implementado) para la contestación de las preguntas por parte de las empresas encuestadas. A este respecto, se encontró:

- **Estrategia corporativa formal de ciberseguridad:**

Una apreciable mayoría (quince (15) respuestas en '0' en la escala de Likert) indicó que, en general, las empresas no cuentan con una estrategia formal de ciberseguridad o manejo de incidentes. Solo una minoría (cuatro (4) en '5' en la escala de Likert y dos (2) en '4' en la escala de Likert) afirma tener implementada dicha estrategia.

Lo anterior, sugiere una vulnerabilidad significativa a nivel sectorial, donde la planificación proactiva en ciberseguridad es escasa y donde se requieren acciones para mejorar la seguridad de la información. Esto se confirma con lo reflejado en los varios ciberataques que ya han sufrido algunas PYMEs y empresas del sector flexográfico y hace necesario tomar prontas y urgentes medidas de protección y de defensa cibernética para asegurar la confiabilidad, la integridad y la disponibilidad de los sistemas informáticos sectoriales.

- **Medidas de seguridad implementadas (antivirus, antimalware):**

Aunque la situación es comparativamente un poco mejor que los resultados obtenidos respecto a una estrategia formal, la encuesta arroja que existe una dispersión considerable. Mientras diez (10) empresas se sitúan en un nivel medio ('3' en la escala de Likert), y cinco (5) afirman tener medidas robustas ('5' en la escala de Likert), un número preocupante (cuatro (4) en '1' en la escala de Likert y una (1) en '0' en la escala de Likert) reporta implementaciones débiles o nulas, resultado que indicó una amplia heterogeneidad en la adopción de herramientas básicas de protección y ciberseguridad a nivel empresarial y sectorial.

- **Personal o departamento de ciberseguridad:**

En este aspecto, los resultados indicaron que una mayoría de las empresas (seis (6) en '0' en la escala de Likert y seis (6) en '1' en la escala de Likert) carecen de personal o de un departamento dedicado o destinado específicamente a la atención de la ciberseguridad empresarial y los resultados revelaron que solo una minoría (tres (3) en '5' en la escala de Likert y cuatro (4) en '4' en la escala de Likert) tiene esta capacidad y dispone de personal especializado en el área de ciberseguridad. La falta de personal dedicado y de talento con experticia en seguridad informática dificultan la gestión efectiva de defensa y protección de la seguridad de la información.

- **Controles de acceso y autenticación robustos y contraseñas seguras:**

En este apartado, los resultados son realmente preocupantes. Una mayoría significativa (trece (13) respuestas en '2' en la escala de Likert) indicó un nivel bajo de adopción de contraseñas seguras y falencias en el uso de autenticación de doble factor (2FA).

Solo dos (2) empresas reportaron un uso robusto ('5' en la escala de Likert). Este resultado representa un riesgo elevado de acceso no autorizado a sistemas informáticos críticos asociados a la gestión de la cadena de producción de la industria flexográfica.

- **Capacitación regular en buenas prácticas de seguridad:**

En este aspecto, los resultados son, nuevamente, de tendencia negativa. La mayoría de las empresas (15 en '0' en la escala de Likert) no ofrece capacitación regular a sus empleados en buenas prácticas de seguridad informática, ni ciberseguridad. La falta de formación, capacitación y concienciación del personal de las empresas es un eslabón débil crítico en la cadena de protección y defensa de la seguridad de la información.

- **Sistema de respaldo (backups):**

En este capítulo, los resultados muestran, una mayor fortaleza relativa, porque si bien, una proporción considerable de empresas (ocho (8) en '5' en la escala de Likert y seis (6) en '4' en la escala de Likert) indicó tener sistemas de respaldo, ya sea físico o en la nube, también, es cierto que no se prueban, no tienen respaldo tipo 3-2-1 y que solo se usan cuando existe la necesidad de realizar recuperación de la información. Sin embargo, un pequeño grupo (Uno (1) en '0' en la escala de Likert) carece de esta medida esencial para la continuidad y resiliencia operativas.

- **Análisis periódico del nivel de riesgo cibernético:**

La mayoría de las empresas (nueve (9) en '0' en la escala de Likert) no realiza análisis de riesgo informático en forma habitual, periódica, frecuente y continuada y esta omisión impide la identificación proactiva y de naturaleza preventiva de vulnerabilidades y la adopción de las medidas de ciberseguridad en un sector crítico de la economía real y máxime considerando el actual panorama de amenazas en constante evolución, sofisticación y complejidad.

- **Compromiso directivo y de la alta gerencia:**

En este aspecto y aunque existe una percepción dividida, sin embargo, se presenta una tendencia que reveló un bajo compromiso directivo, pues mientras seis (6) empresas indicaron un alto compromiso directivo ('5' en la escala de Likert), también, es de considerar que un número similar (siete (7) en '1' en la escala de Likert y dos (2) en '0' en la escala de Likert) señalaron un bajo

involucramiento del staff gerencial, denotando un problema de apoyo de parte de la alta dirección que impregna una gran parte del sector flexográfico, y donde es fundamental impulsar una cultura de ciberseguridad.

- **Maquinaria o equipos de línea de producción con conexión a internet o a redes externas:**

La mayoría de las empresas (ocho (8) en '1' en la escala de Likert y cinco (5) en '2' en la escala de Likert) reportan tener equipos de producción con algún tipo de conectividad, aunque no necesariamente permanente o extensa y esto introduce potenciales vectores de ataque adicionales que deben ser gestionados para una adecuada gestión de defensa y protección de la seguridad de la información. Al respecto, debe notarse que cinco (5) empresas (con puntaje de '5' en la escala de Likert) indicaron una conectividad significativa y permanente de su infraestructura informática asociada a la gestión de la cadena de producción, con el ciberespacio (internet).

- **Incidentes o ataques informáticos en el pasado:**

Uno de los hallazgos más alarmantes consistió en que una gran mayoría de las empresas encuestadas (veintiuno (21) con respuestas en '5' en la escala de Likert) confirmaron ya haber sufrido incidentes o ataques informáticos en el pasado y, aun cuando, la encuesta no entró en pormenores sobre la cantidad, frecuencia, tipo, naturaleza e impactos de los ciberataques sufridos de manera específica (Si se confirmó, de manera informal, por parte de los autores que algunas empresas han sufrido ataques de ransomware con pérdidas económicas y de información para las empresas víctimas, algunas de ellas no pagaron el rescate exigido y otras, por lo menos una compañía, si lo hizo, aunque no se supo el monto del valor pagado), los resultados si subrayan la realidad de las ciberamenaza y la necesidad urgente de mejorar las defensas ante la realidad que el sector es blanco de potencial interés de parte de los ciberatacantes.

En este sentido, solo cuatro (4) empresas (con puntaje '0' en la escala de Likert) indicaron no haber sufrido ciberincidentes.

- **Equipo computacional viejo y obsoleto:**

Aun cuando, en este punto, los resultados obtenidos son mixtos, debe resaltarse que no sorprendieron, pues se esperaba, por parte de los autores, corroborar la obsolescencia de las infraestructuras informáticas y computacionales asociadas a la gestión de las cadenas de producción de la industria flexográfica y los resultados así lo reflejaron, pues se identificó una tendencia marcada y preocupante hacia el uso de tecnología obsoleta por parte de las PYMEs y empresas del sector. En efecto, mientras siete (7) empresas se sitúan en un nivel medio (con valoración '2' en la escala de Likert), un número considerable de compañías (tres (3) en '0' en la escala de Likert y tres (3) en '1' en la escala de Likert) indicaron tener equipos actualizados, pero, otro grupo importante (siete (7) en '3' en la escala de Likert, dos (2) en '4' y tres (3) en '5' en la escala de Likert) reconocieron el uso de equipos viejos, antiguos y muy obsoletos.

Como es de público conocimiento, el hardware y software obsoletos son mucho más vulnerables y amplían la superficie de ataque, incrementando la exposición al riesgo informático y planteando vulnerabilidades potencialmente susceptibles de ser explotadas por medio ciberataques y amenazas maliciosas y esto constituye una gran preocupación de seguridad informática para PYMEs y empresas del sector.

- **Sistemas operativos utilizados en equipos computacionales asociados a la gestión de la cadena de producción esencial del sector flexográfico:**

A continuación, se presenta un resumen analítico de los sistemas operativos hallados para la gestión y control de las cadenas de producción del sector flexográfico y de sus consecuencias y significancia a efectos de esta tesis de maestría:

- **Windows 11:**

Este sistema operativo tiene una presencia significativa (diez y siete (17) instancias) en el sector flexográfico, en la actualidad.

- **Windows 10:**

Es el sistema operativo predominante (diez y ocho (18) instancias) en el sector flexográfico, en la actualidad.

- **Windows 8:**

Se encontró una presencia nula (ninguna (0) instancia reportada en la encuesta) en el sector flexográfico, en la actualidad, lo cual es positivo dado su obsolescencia y falta de soporte.

- **Windows 7:**

Preocupa su persistencia (once (11) instancias) en el sector flexográfico, en la actualidad, ya que es un sistema operativo sin soporte y con vulnerabilidades ampliamente conocidas.

- **Windows XP:**

Su presencia es nula (ninguna (0) instancia reportada en la encuesta) en el sector flexográfico, en la actualidad, lo cual es positivo dado su obsolescencia y falta de soporte.

- **Linux:**

Su uso es nulo (ninguna (0) instancia reportada en la encuesta) en el sector flexográfico, en la actualidad.

- **MacOS:**

Su uso es nulo (ninguna (0) instancia reportada en la encuesta) en el sector flexográfico, en la actualidad.

De lo anterior, se desprende que, la presencia de Windows 7 es un riesgo de seguridad importante que, debe abordarse con urgencia mediante la actualización a versiones más recientes y seguras. Igualmente, se recomienda, desde ya, la transición a Windows 11, pues su soporte (incluidas actualizaciones y parcheos de seguridad) ha de terminar, por parte de Microsoft Corporation, en fecha que esta ad-portal, muy seguramente, para octubre de este año que corre (2025).

Análisis DOFA derivado de los resultados del instrumento aplicado.

Así pues, los resultados y su análisis contextualizan el estado actual y los requerimientos de ciberseguridad en el sector flexográfico que, según el panorama de los resultados arrojados por la encuesta, revelan la presencia de deficiencias significativas que requieren atención inmediata. A continuación, se presentan las principales fortalezas, debilidad oportunidad y amenazas que se han reflejado del modelo y que orientaron la consolidación del modelo de ciberseguridad desarrollado en esta tesis de maestría, a saber:

- **Fortalezas relativas:**

- La adopción de sistemas de respaldo (backups) parece ser el área mejor gestionada por una porción importante de PYMEs y empresas del sector.
- Medidas de ciberseguridad, aunque incipientes (Antivirus).

- **Debilidades críticas:**

- Ausencia generalizada de estrategias formales de ciberseguridad y de personal dedicado a la gestión de la ciberseguridad.
- Baja adopción de controles de acceso adecuados, como uso de contraseñas robustas y seguras y de autenticación de doble factor.
- Falta casi total de concientización, capacitación y entrenamiento del personal corporativo sectorial en buenas prácticas de seguridad. Carencia de actualizaciones permanentes en este campo.
- Omisión generalizada de análisis y evaluación periódica de riesgo informático.
- Alta incidencia de ataques informáticos previos, lo que confirma la exposición al riesgo de las PYMEs y empresas del sector flexográfico.

- Presencia preocupante de sistemas operativos obsoletos (Windows 7) en equipos vinculados a la gestión de la cadena de producción de las PYMEs y empresas del sector flexográfico.
- **Áreas de Oportunidad:**
 - **Compromiso directivo:**

Es fundamental elevar el nivel de compromiso y liderazgo a nivel directivo y gerencial para asegurar la adecuada asignación de recursos y definir las estrategias corporativas necesarias. Esto solo se logra haciendo caer en la cuenta al staff directivo respecto a que la ciberseguridad, en la actualidad, es una asunto tan importante y vital para las empresas y organizaciones, como lo son los aspectos financieros, tributarios, comerciales, legales, de producción, etc.
 - **Concientización y capacitación:**

Es fundamental fomentar la concientización, implementando programas de formación, capacitación y entrenamiento para todo el personal de la organización y, en general, sobre ciberseguridad y seguridad informática, pero, en particular, sobre los riesgos cibernéticos y las buenas prácticas de seguridad informática para asegurar que el personal no padezca por ignorancia, omisión o negligencia.
 - **Planificación estratégica:**

Desarrollar e implementar estrategias formales de ciberseguridad adaptadas a las necesidades y recursos de cada PYME o empresa del sector.
 - **Fortalecimiento de controles básicos:**

Implementar medidas esenciales como antivirus actualizados, firewalls, contraseñas seguras y, fundamentalmente un estricto control de acceso con concesión de mínimos privilegios y confianza nula (Zero trust).
 - **Gestión de vulnerabilidades:**

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica.

Realizar revisiones, sino auditorías, de seguridad y análisis y evaluación del riesgo informático de manera periódica, continuada y disciplinada, en aras de identificar y mitigar vulnerabilidades, incluyendo y, particularmente considerando, la actualización de software y hardware obsoleto.

- **Modernización de sistemas operativos:**

Migrar urgentemente los sistemas operativos a sus versiones más modernas y actualizadas, incluyendo equipos con versiones anteriores de Windows (10 y 7) para garantizar versiones más seguras y con soporte y actualizaciones activas y disponibles.

Matriz DOFA – Diagnóstico de Ciberseguridad del Sector Flexográfico 2025	
Fortalezas (F)	Debilidades (D)
F1. Presencia significativa de sistemas de respaldo y copias de seguridad.	D1. Ausencia generalizada de estrategias formales de ciberseguridad e incident response.
	D2. Carencia de personal o departamentos especializados en ciberseguridad.
F2. Algunas empresas reportan uso de medidas antivirus y antimalware robustas.	D3. Falta de implementación de controles de acceso seguros y autenticación multifactor.
	D4. Casi total ausencia de programas de capacitación y concienciación en ciberseguridad.
F3. Un grupo reducido de empresas cuenta con compromiso directivo visible.	D5. No se realizan análisis periódicos de riesgo cibernético.
	D6. Uso persistente de sistemas operativos obsoletos (Windows 7).
F4. Algunas compañías utilizan sistemas operativos actualizados (Windows 10/11).	D7. Alta heterogeneidad en la adopción de prácticas de ciberseguridad básica.
Oportunidades (O)	Amenazas (A)
O1. Incrementar el compromiso directivo mediante sensibilización sobre riesgos.	A1. Alta incidencia de ciberataques previos, incluyendo casos de ransomware con pérdidas significativas.
O2. Disponibilidad de normas y marcos internacionales como NIST, ISO 27001, etc.	A2. Equipos de producción conectados a redes e internet sin protección adecuada.
O3. Posibilidad de formación continua mediante alianzas con entidades académicas.	A3. Obsolescencia tecnológica como superficie de ataque activa.
O4. Modernización de sistemas operativos y migración a tecnologías más seguras.	A4. Entorno de amenazas en evolución constante y creciente sofisticación de los ciberataques.
O5. Aplicación de políticas sectoriales de ciberseguridad con apoyo estatal.	A5. Bajo nivel de cultura de ciberseguridad generalizado en el sector.

Fig. A1.13

Matriz DOFA resultante del análisis de la encuesta de diagnóstico del estado y requerimientos de seguridad de la información en el sector flexográfico 2025.

Nota: Fortalezas, Debilidades, Oportunidades y Amenazas cibernéticas encontradas. Fuente: Autoría propia.

Los anteriores puntos constituyen una base sólida de mejoramiento de la seguridad informática sectorial y pueden considerarse y adoptarse como requerimientos urgentes para la consolidación del diseño de un modelo de ciberseguridad para las infraestructuras informáticas y computacionales asociadas a la gestión de la cadena productiva crítica del sector flexográfico.

En resumen, el sector flexográfico se enfrenta a un entorno de amenazas cibernéticas con una preparación general que, acorde con los resultados obtenidos, se refleja insuficiente, pues si bien existen focos de buenas prácticas e intentos aislados de formalización estratégica y mejoramiento, la mayoría de las PYMEs y empresas encuestadas, presentan vulnerabilidades importantes en múltiples frentes, lo cual hace imperativo, que se tomen medidas proactivas e inmediatas para fortalecer la defensa cibernética, a fin de proteger la seguridad de la información, en particular, la confiabilidad, la integridad y la disponibilidad, de las infraestructuras computacionales asociadas a la gestión de las cadenas de producción críticas de PYMEs y empresas del sector flexográfico, asegurando así, la continuidad y resiliencia de sus operaciones, cuyo funcionamiento normal es esencial para la sociedad, la economía y el país entero.

Autodiagnósticos derivados de los resultados del instrumento aplicado

A este respecto, los resultados anteriores y su análisis sirvieron como base sólida para elaborar los siguientes autodiagnósticos y consolidar, tanto necesidades y requerimientos de seguridad informática como, también, para conocer el estado actual de la industria flexográfica en este campo, con la finalidad de consolidar la información necesaria para realizar el análisis y la evaluación del riesgo cibernético, a través de la herramienta de autodiagnóstico respectiva. Al efecto, se implementaron dos (2) diferentes autoevaluaciones, una bajo los estándares y lineamientos de la norma ISO 27001 y otro bajo las directrices del marco NIST 2.0 CSF, a saber:

- **Autodiagnóstico de seguridad de la información en la industria flexográfica según la norma ISO 27001**

El autodiagnóstico, presentado en detalle, en el Anexo Nro. 3 de esta tesis de maestría (ver Anexo Nro. 3), y cuyos aspectos más relevantes se consignan a continuación, permitió evaluar el estado de la seguridad de la información en la industria flexográfica y sus necesidades y requerimientos de ciberseguridad. De otra parte, su implementación se basó en los resultados de la encuesta “Diagnóstico del estado actual de la seguridad de la información en el sector flexográfico” realizada a Treinta (30) empresas del sector bajo los lineamientos de la norma ISO 27001.

Tabla A1.1

Autodiagnóstico del sector flexográfico según la norma ISO 27001.

POLÍTICAS DE SEGURIDAD					
Existen documento(s) de políticas de seguridad de SI	☐	FALSO	0		
Existe normativa relativa a la seguridad de los SI	☐	FALSO	0		
Existen procedimientos relativos a la seguridad de SI	☐	FALSO	0		
Existe un responsable de las políticas, normas y procedimientos	☐	FALSO	0		
Existen mecanismos para la comunicación a los usuarios de las normas	☐	FALSO	0		
Existen controles regulares para verificar la efectividad de las políticas	☐	FALSO	0	si	no
ORGANIZACIÓN DE LA SEGURIDAD			0	0,00	100,00
Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	☐	FALSO	0		
Existe un responsable encargado de evaluar la adquisición y cambios de SI	☐	FALSO	0		
La Dirección y las áreas de la Organización participan en temas de seguridad	☐	FALSO	0		
Existen condiciones contractuales de seguridad con terceros y outsourcing	☐	FALSO	0		
Existen criterios de seguridad en el manejo de terceras partes	☐	FALSO	0		
Existen programas de formación en seguridad para los empleados, clientes y terceros	☐	FALSO	0		
Existe un acuerdo de confidencialidad de la información que se accesa.	☐	FALSO	0		
Se revisa la organización de la seguridad periódicamente por una empresa externa	☐	FALSO	0	si	no
ADMINISTRACIÓN DE ACTIVOS			0	0,00	100,00
Existen un inventario de activos actualizado	☐	FALSO	0		
El Inventario contiene activos de datos, software, equipos y servicios	☐	FALSO	0		
Se dispone de una clasificación de la información según la criticidad de la misma	☐	FALSO	0		
Existe un responsable de los activos	☐	FALSO	0		
Existen procedimientos para clasificar la información	☐	FALSO	0		
Existen procedimientos de etiquetado de la información	☐	FALSO	0	si	no
SEGURIDAD DE LOS RRHH			0	0,00	100,00
Se tienen definidas responsabilidades y roles de seguridad	☐	FALSO	0		
Se tiene en cuenta la seguridad en la selección y baja del personal	☐	FALSO	0		
Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	☐	FALSO	0		
Se imparte la formación adecuada de seguridad y tratamiento de activos	☐	FALSO	0		
Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	☐	FALSO	0		
Se recogen los datos de los incidentes de forma detallada	☐	FALSO	0		
Informan los usuarios de las vulnerabilidades observadas o sospechadas	☐	FALSO	0		
Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	☐	FALSO	0	si	no
Existe un proceso disciplinario de la seguridad de la información	☐	FALSO	0		
SEGURIDAD FÍSICA Y DEL AMBIENTE			0	0,00	100,00

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica.

SEGURIDAD FÍSICA Y DEL AMBIENTE		0	0,00	100,00
Existe perímetro de seguridad física (una pared, puerta con llave)	☒ VERDADERO	1		
Existen controles de entrada para protegerse frente al acceso de personal no autorizado	☒ VERDADERO	1		
El área segura esta cerrada, aislada y protegida de eventos naturales	☒ VERDADERO	1		
En las áreas seguras existen controles adicionales al personal propio y ajeno	☒ VERDADERO	1		
Las áreas de carga y expedición están aisladas de las áreas de SI	☐ FALSO	0		
La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	☐ FALSO	0		
Existen protecciones frente a fallos en la alimentación eléctrica	☐ FALSO	0		
Existe seguridad en el cableado frente a daños e interceptaciones	☐ FALSO	0		
Se asegura la disponibilidad e integridad de todos los equipos	☐ FALSO	0		
Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	☐ FALSO	0		
Se incluye la seguridad en equipos móviles	☐ FALSO	0		
GESTIÓN DE COMUNICACIONES Y OPERACIONES		4	36,36	63,64
Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados	☐ FALSO	0		
Están establecidas responsabilidades para controlar los cambios en equipos	☐ FALSO	0		
Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	☐ FALSO	0		
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	☐ FALSO	0		
Existe una separación de los entornos de desarrollo y producción	☐ FALSO	0		
Existen contratistas externos para la gestión de los Sistemas de Información	☒ VERDADERO	1		
Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento	☐ FALSO	0		
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	☐ FALSO	0		
Controles contra software maligno	☐ FALSO	0		
Realizar copias de backup de la información esencial para el negocio	☒ VERDADERO	1		
Existen logs para las actividades realizadas por los operadores y administradores	☐ FALSO	0		
Existen logs de los fallos detectados	☐ FALSO	0		
Existen rastro de auditoría	☐ FALSO	0		
Existe algún control en las redes	☒ VERDADERO	1		
Hay establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)	☐ FALSO	0		
Eliminación de los medios informáticos. Pueden disponer de información sensible	☐ FALSO	0		
Existe seguridad de la documentación de los Sistemas	☐ FALSO	0		
Existen acuerdos para intercambio de información y software	☐ FALSO	0		
Existen medidas de seguridad de los medios en el tránsito	☐ FALSO	0		
Existen medidas de seguridad en el comercio electrónico.	☐ FALSO	0		
Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	☐ FALSO	0	si	no
Existen medidas de seguridad en las transacciones en línea	☐ FALSO	0		
Se monitorean las actividades relacionadas a la seguridad	☐ FALSO	0		
CONTROL DE ACCESOS		3	15,00	85,00
Existe una política de control de accesos	☐ FALSO	0		
Existe un procedimiento formal de registro y baja de accesos	☐ FALSO	0		
Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	☒ VERDADERO	1		
Existe una gestión de los password de usuarios	☒ VERDADERO	1		
Existe una revisión de los derechos de acceso de los usuarios	☐ FALSO	0		
Existe el uso del password	☒ VERDADERO	1		
Se protege el acceso de los equipos desatendidos	☐ FALSO	0		
Existen políticas de limpieza en el puesto de trabajo	☐ FALSO	0		
Existe una política de uso de los servicios de red	☐ FALSO	0		
Se asegura la ruta (path) desde el terminal al servicio	☐ FALSO	0		
Existe una autenticación de usuarios en conexiones externas	☐ FALSO	0		
Existe una autenticación de los nodos	☐ FALSO	0		
Existe un control de la conexión de redes	☒ VERDADERO	1		
Existe un control del routing de las redes	☐ FALSO	0		
Existe una identificación única de usuario y una automática de terminales	☒ VERDADERO	1		
Existen procedimientos de log-on al terminal	☐ FALSO	0		
Se ha incorporado medidas de seguridad a la computación móvil	☐ FALSO	0		
Está controlado el teletrabajo por la organización	☐ FALSO	0	si	no
DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS		5	31,25	68,75
Se asegura que la seguridad está implantada en los Sistemas de Información	☐ FALSO	0		
Existe seguridad en las aplicaciones	☐ FALSO	0		
Existen controles criptográficos.	☐ FALSO	0		
Existe seguridad en los archivos de los sistemas	☐ FALSO	0		
Existe seguridad en los procesos de desarrollo, testing y soporte	☐ FALSO	0	si	no
Existen controles de seguridad para los resultados de los sistemas	☐ FALSO	0		
Existe la gestión de los cambios en los SO.	☐ FALSO	0		
Se controlan las vulnerabilidades de los equipos	☐ FALSO	0		
ADMINISTRACIÓN DE INCIDENTES		0	0,00	100,00
Se comunican los eventos de seguridad	☐ FALSO	0		
Se comunican los debilidades de seguridad	☐ FALSO	0		
Existe definidas las responsabilidades ante un incidente.	☐ FALSO	0		
Existe un procedimiento formal de respuesta	☐ FALSO	0		
Existe la gestión de incidentes	☐ FALSO	0		
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		0	0,00	100,00
Existen procesos para la gestión de la continuidad.	☐ FALSO	0		
Existe un plan de continuidad del negocio y análisis de impacto	☐ FALSO	0		
Existe un diseño, redacción e implantación de planes de continuidad	☐ FALSO	0		
Existe un marco de planificación para la continuidad del negocio	☐ FALSO	0		
Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	☐ FALSO	0	si	no
CUMPLIMIENTO		0	0,00	100,00
Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	☐ FALSO	0		
Existe el resguardo de la propiedad intelectual	☐ FALSO	0		
Existe el resguardo de los registros de la organización	☐ FALSO	0		
Existe una revisión de la política de seguridad y de la conformidad técnica	☐ FALSO	0		
Existen consideraciones sobre las auditorías de los sistemas	☐ FALSO	0		
TOTALES		0	0,00	100,00

Nota: Autodiagnóstico del sector flexográfico según la norma ISO 27001 (ver Anexo Nro.3). Fuente: Autoría propia.

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño
Maestría en Seguridad Informática
I.T.M.

Al efecto, en esta autoevaluación inicial, se analizaron aspectos fundamentales del estado de la seguridad de la información sectorial y su alineación con la norma ISO 27001, lo cual constituyó una fuente de información clave para concebir una idea aproximada de la naturaleza y requerimientos de modelo de ciberseguridad requerido para el sector flexográfico.

RESULTADOS AUTODIAGNÓSTICO GENERAL

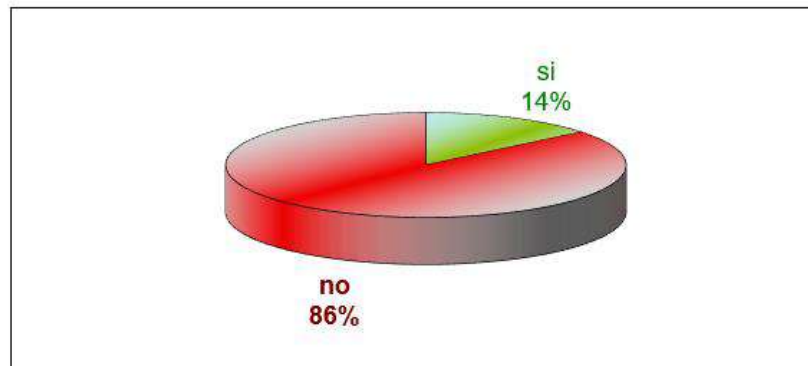


Fig. A1.14

Resultado general del autodiagnóstico del sector flexográfico según la norma ISO 27001.

Nota: Resultado general del autodiagnóstico del sector flexográfico según la norma ISO 27001. Fuente: Autoría propia.

POLÍTICAS DE SEGURIDAD	ORGANIZACIÓN DE LA SEGURIDAD												
<table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>si</td> <td>0%</td> </tr> <tr> <td>no</td> <td>100%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	si	0%	no	100%	<table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>si</td> <td>0%</td> </tr> <tr> <td>no</td> <td>100%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	si	0%	no	100%
Respuesta	Porcentaje												
si	0%												
no	100%												
Respuesta	Porcentaje												
si	0%												
no	100%												
CLASIFICACIÓN Y CONTROL DE ACTIVOS	SEGURIDAD DEL PERSONAL												
<table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>si</td> <td>0%</td> </tr> <tr> <td>no</td> <td>100%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	si	0%	no	100%	<table border="1"> <thead> <tr> <th>Respuesta</th> <th>Porcentaje</th> </tr> </thead> <tbody> <tr> <td>si</td> <td>0%</td> </tr> <tr> <td>no</td> <td>100%</td> </tr> </tbody> </table>	Respuesta	Porcentaje	si	0%	no	100%
Respuesta	Porcentaje												
si	0%												
no	100%												
Respuesta	Porcentaje												
si	0%												
no	100%												

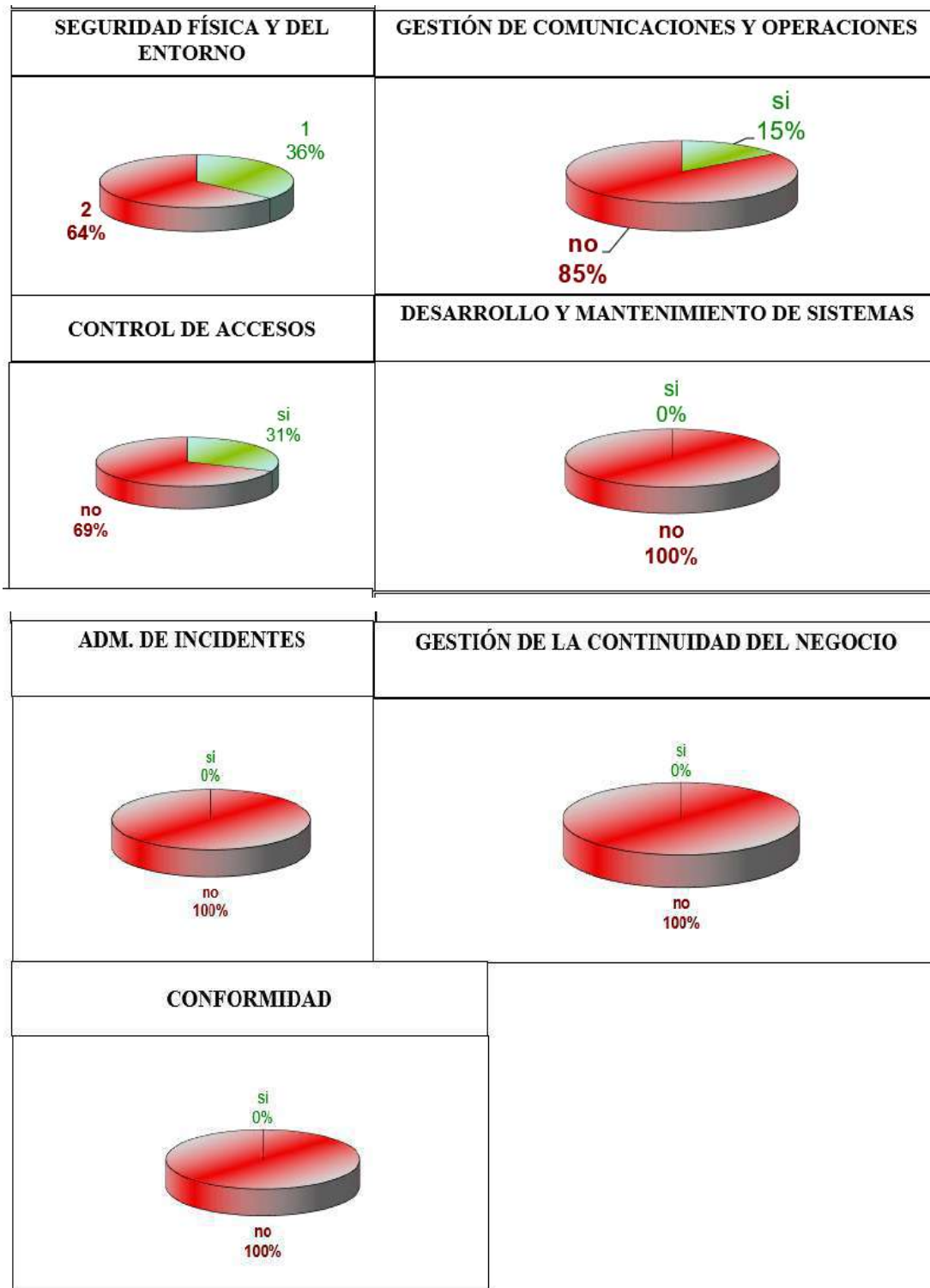


Fig. A1.15

Resultado del autodiagnóstico del sector flexográfico por áreas según la norma ISO 27001.

Nota: Resultado del autodiagnóstico del sector flexográfico por áreas según la norma ISO 27001 (ver Anexo Nro. 3).

Fuente: Autoría propia.

Debe anotarse, que el autodiagnóstico según la norma ISO 27001, igual que el caso anterior (NIST 2.0 CSF), consta de dos (2) etapas, una primera fase que evalúa el estado actual y una segunda etapa que evalúa el estado de la infraestructura o sistema informático una vez implementados los respectivos controles. Esta segunda parte del autodiagnóstico se efectuará en la fase 3 de verificación o validación del modelo de ciberseguridad desarrollado en esta tesis de maestría.

- **Autodiagnóstico de seguridad de la información en la Industria flexográfica según el marco NIST 2.0 CSF**

El autodiagnóstico, presentado a continuación, en sus aspectos más relevantes y que puede observarse en mayor detalle, en el Anexo Nro. 3 de esta tesis de maestría (ver Anexo Nro. 3 para mayor detalle), evaluó el estado de la seguridad de la información en la industria flexográfica y sus necesidades y requerimientos de ciberseguridad. De otra parte, su implementación se basó en los resultados de la encuesta “Diagnóstico del estado actual de la seguridad de la información en el sector flexográfico” realizada a Treinta (30) empresas del sector bajo los lineamientos del marco NIST 2.0 CSF.

Al efecto, en esta autoevaluación inicial, se analizaron aspectos fundamentales del estado de la seguridad de la información sectorial y su alineación con el marco NIST 2.0 CSF, al igual que se realizó, en el caso anterior, con la autoevaluación según los lineamientos de la norma ISO 27001, y esto constituyó una fuente de información clave para concebir una idea aproximada, pero, bastante fidedigna de la naturaleza, condiciones y requerimientos para un modelo de ciberseguridad como el requerido para el sector flexográfico y presentado en esta tesis de maestría.

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica.

Tabla A1.2

Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función gobernar.

AUTODIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DEL SECTOR FLEXOGRAFICO SEGÚN MARCO NIST 2.0 CSF			Perfil actual	
FUNCIÓN	CATEGORÍA	SUBCATEGORÍA	Estado	Nivel
Gobernar (GV): Se establecen, comunican y supervisan la estrategia, las expectativas y la política de gestión de riesgos de seguridad cibernética de la organización.	Contexto organizativo (GV.OC): Se comprenden las circunstancias - misión, expectativas de las partes interesadas, dependencias y requisitos legales, normativos y contractuales - que afectan a las decisiones de gestión de riesgos de seguridad cibernética de la organización	GV.OC-01: Se comprende la misión de la organización y se informa sobre la gestión de riesgos de seguridad cibernética.	No hay roles ni responsabilidades bien definidos en el equipo de TI y seguridad. El personal no tiene claro quién debe gestionar incidentes o riesgos.	Nivel 1 Parcial
		GV.OC-02: Las partes interesadas internas y externas son comprendidas, y sus necesidades y expectativas con respecto a la gestión de riesgos de seguridad cibernética son comprendidas y consideradas.	No existen roles ni responsabilidades respecto a ciberseguridad.	Nivel 1 Parcial
		GV.OC-03: Se comprenden y gestionan los requisitos legales, normativos y contractuales relativos a la seguridad cibernética, incluidas las obligaciones en materia de privacidad y libertades civiles.	No existe evidencia, no tienen roles, responsables.	Nivel 1 Parcial
		GV.OC-04: Se comprenden y comunican los objetivos, las capacidades y los servicios críticos de los que dependen las partes interesadas externas o que esperan de la organización.	No se comunica porque no existen objetivos, planes.	Nivel 1 Parcial
		GV.OC-05: Se comprenden y comunican los resultados, capacidades y servicios de los que depende la organización.	No existe evidencia.	Nivel 1 Parcial
	Estrategia de gestión de riesgos (GV.RM): Se establecen, comunican y utilizan las prioridades, las restricciones, las declaraciones de tolerancia y apetito por el riesgo y los supuestos de la organización para respaldar las decisiones sobre el riesgo operativo	GV.RM-01: Los objetivos de la gestión de riesgos son establecidos y acordados por las partes interesadas de la organización.	No hay roles ni responsabilidades bien definidos en el equipo de TI y seguridad, ni con los proveedores tecnológicos.	Nivel 1 Parcial
		GV.RM-02: Se establecen, se comunican y se mantienen las declaraciones sobre el apetito de riesgo y la tolerancia al riesgo.	No existe evidencia, no evalúan en riesgo.	Nivel 1 Parcial
		GV.RM-03: Las actividades y los resultados de la gestión de riesgos de seguridad cibernética se incluyen en los procesos de gestión de riesgos de la empresa.	No existe evidencias.	Nivel 1 Parcial
		GV.RM-04: Se establece y comunica una dirección estratégica que describe las opciones adecuadas de respuesta al riesgo.	No existe evidencias.	Nivel 1 Parcial
		GV.RM-05: Se establecen líneas de comunicación en toda la organización para los riesgos de seguridad cibernética, lo que incluye a los riesgos de proveedores y otros terceros.	No existe evidencias.	Nivel 1 Parcial
		GV.RM-06: Se establece y comunica un método estandarizado para calcular, documentar, categorizar y priorizar los riesgos de seguridad cibernética.	No existe evidencias.	Nivel 1 Parcial
		GV.RM-07: Se caracterizan las oportunidades estratégicas (es decir, los riesgos positivos) y se incluyen en las discusiones sobre riesgos de seguridad cibernética de la organización.	No existe evidencias.	Nivel 1 Parcial
	Funciones, responsabilidades y autoridades (GV.RR): Se establecen y comunican las funciones, las responsabilidades y las competencias en materia de seguridad cibernética para fomentar la rendición de cuentas, la evaluación del desempeño y la mejora continua.	GV.RR-01: El liderazgo organizativo es responsable de los riesgos de seguridad cibernética y fomenta una cultura consciente de los riesgos, ética y de mejora continua.	No existe evidencias.	Nivel 1 Parcial
		GV.RR-02: Se establecen, comunican, comprenden y aplican las funciones, responsabilidades y autoridades relacionadas con la gestión de riesgos de seguridad cibernética.	No existe evidencias.	Nivel 1 Parcial
		GV.RR-03: Se asignan recursos adecuados de acuerdo con la estrategia de riesgos de seguridad cibernética, las funciones, las responsabilidades y las políticas.	No existe evidencias.	Nivel 1 Parcial
		GV.RR-04: La seguridad cibernética se incluye en las prácticas de recursos humanos.	No existe evidencias.	Nivel 1 Parcial
	Política (GV.PO): La política de seguridad cibernética de la organización es establecida, comunicada y aplicada.	GV.PO-01: La política de gestión de riesgos de seguridad cibernética se establece en base al contexto organizativo, la estrategia de seguridad cibernética y las prioridades, y es comunicada y aplicada.	No existe evidencias.	Nivel 1 Parcial
		GV.PO-02: La política de gestión de riesgos de seguridad cibernética se revisa, actualiza, comunica y aplica para reflejar los cambios de los requisitos, las amenazas, la tecnología y la misión de la organización.	No existe evidencias.	Nivel 1 Parcial
	Supervisión (GV.OV): Los resultados de las actividades de gestión de riesgos de seguridad cibernética en toda la organización y el rendimiento se utilizan para informar, mejorar y ajustar la estrategia de gestión de riesgos.	GV.OV-01: Los resultados de la estrategia de gestión de riesgos de seguridad cibernética se revisan para informar y ajustar la estrategia y la dirección.	No existe evidencias.	Nivel 1 Parcial
		GV.OV-02: La estrategia de gestión de riesgos de seguridad cibernética se revisa y ajusta para garantizar la cobertura de los requisitos y riesgos de la organización.	No existe evidencias.	Nivel 1 Parcial
		GV.OV-03: El rendimiento de la gestión de riesgos de seguridad cibernética de la organización se evalúa y revisa para realizar los ajustes necesarios.	No existe evidencias.	Nivel 1 Parcial
	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética (GV.SC): Las partes interesadas de la organización identifican, establecen, gestionan, supervisan y mejoran los procesos de gestión de riesgos de la cadena de suministro cibernética.	GV.SC-01: Las partes interesadas de la organización establecen y acuerdan un programa, estrategia, objetivos, políticas y procesos de gestión de riesgos de seguridad cibernética en la cadena de suministro.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-02: Se establecen, comunican y coordinan interna y externamente las funciones y responsabilidades de seguridad cibernética para proveedores, clientes y colaboradores.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-03: La gestión de riesgos de la cadena de suministro de seguridad cibernética está integrada en la seguridad cibernética y la gestión de riesgos empresariales, la evaluación de riesgos y los procesos de mejora.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-04: Los proveedores son conocidos y priorizados por criticidad.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-05: Los requisitos para abordar los riesgos de seguridad cibernética en las cadenas de suministro se establecen, priorizan e integran en contratos y otros tipos de acuerdos con proveedores y otras terceras partes pertinentes.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-06: Se llevan a cabo la planificación y la diligencia debida para reducir los riesgos antes de entablar relaciones formales con proveedores u otros terceros.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-07: Los riesgos planteados por un proveedor, sus productos y servicios y otros terceros se comprenden, registran, priorizan, evalúan, responden y monitorean a lo largo de la relación.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-08: Los proveedores pertinentes y otros terceros se incluyen en las actividades de planificación, respuesta y recuperación de incidentes.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-09: Las prácticas de seguridad de la cadena de suministro se integran en los programas de seguridad cibernética y de gestión de riesgos empresariales, y su rendimiento se monitorea a lo largo del ciclo de vida de los productos y servicios tecnológicos.	No existe evidencias.	Nivel 1 Parcial
		GV.SC-10: Los planes de gestión de riesgos de la cadena de suministro de seguridad cibernética incluyen disposiciones para las actividades que ocurren después de la conclusión de un acuerdo de colaboración o servicio.	No existe evidencias.	Nivel 1 Parcial

Nota: Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CS (ver Anexo Nro. 3). Función Gobernar. Fuente: Autoría propia.

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica.

Tabla A1.3

Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función identificar.

Identificar (ID): Se conocen los riesgos de seguridad cibernética actuales de la organización.	Gestión de activos (ID.AM): Los activos (p. ej., datos, hardware, software, sistemas, instalaciones, servicios, personas) que permitan a la organización alcanzar sus objetivos empresariales se identifican y gestionan de acuerdo con su importancia relativa para los objetivos organizativos y la estrategia de riesgo de la organización.	ID.AM-01: Se mantienen inventarios del hardware gestionado por la organización.	No existe evidencias	Nivel 1 Parcial
		ID.AM-02: Se mantienen inventarios de software, servicios y sistemas gestionados por la organización.	No existe evidencias	Nivel 1 Parcial
		ID.AM-03: Se mantienen representaciones de la comunicación de red autorizada de la organización y de los flujos de datos de red internos y externos.	No existe evidencias	Nivel 1 Parcial
		ID.AM-04: Se mantienen inventarios de los servicios prestados por los proveedores.	No existe evidencias	Nivel 1 Parcial
		ID.AM-05: Se priorizan los activos en función de su clasificación, criticidad, recursos e impacto en la misión.	No existe evidencias	Nivel 1 Parcial
		ID.AM-07: Se mantienen inventarios de datos y los metadatos correspondientes para los tipos de datos designados.	No existe evidencias	Nivel 1 Parcial
		ID.AM-08: Los sistemas, el hardware, el software, los servicios y los datos se gestionan durante todo su ciclo de vida.	No existe evidencias	Nivel 1 Parcial
		ID.RA-01: Se identifican, validan y registran las vulnerabilidades de los activos.	No existe evidencias	Nivel 1 Parcial
		ID.RA-02: Se recibe información sobre amenazas cibernéticas de foros y fuentes de intercambio de información.	No existe evidencias	Nivel 1 Parcial
		ID.RA-03: Se identifican y registran las amenazas internas y externas a la organización.	No existe evidencias	Nivel 1 Parcial
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para la organización, los activos y los individuos.	ID.RA-04: Se identifican y registran los impactos potenciales y las probabilidades de que las amenazas exploten las vulnerabilidades.	No existe evidencias	Nivel 1 Parcial
		ID.RA-05: Las amenazas, las vulnerabilidades, las probabilidades y los impactos se utilizan para comprender el riesgo inherente e informar sobre la orientación de la respuesta al riesgo.	No existe evidencias	Nivel 1 Parcial
		ID.RA-06: Se eligen, priorizan, planifican, controlan y comunican las respuestas al riesgo.	No existe evidencias	Nivel 1 Parcial
		ID.RA-07: Se gestionan los controles y las excepciones, se evalúa su impacto en el riesgo, se registran y se realiza su seguimiento.	No existe evidencias	Nivel 1 Parcial
		ID.RA-08: Se establecen procesos para recibir, analizar y responder a las divulgaciones de vulnerabilidades.	No existe evidencias	Nivel 1 Parcial
		ID.RA-09: Se evalúa la autenticidad e integridad del hardware y software antes de su adquisición y uso.	No existe evidencias	Nivel 1 Parcial
		ID.RA-10: Se evalúan los proveedores críticos antes de su adquisición.	No existe evidencias	Nivel 1 Parcial
	Mejora (ID.IM): Se identifican mejoras en los procesos, procedimientos y actividades de gestión de riesgos de seguridad cibernética de la organización en todas las funciones del CSF.	ID.IM-01: Las mejoras se identifican a partir de evaluaciones.	No existe evidencias	Nivel 1 Parcial
		ID.IM-02: Las mejoras se identifican a partir de pruebas y ejercicios de seguridad, lo que incluye a los realizados en coordinación con proveedores y terceros pertinentes.	No existe evidencias	Nivel 1 Parcial
		ID.IM-03: Las mejoras se identifican a partir de la ejecución de procesos, procedimientos y actividades operativas.	No existe evidencias	Nivel 1 Parcial
		ID.IM-04: Se establecen, comunican, mantienen y mejoran los planes de respuesta a incidentes y otros planes de seguridad cibernética que afectan a las operaciones.	No existe evidencias	Nivel 1 Parcial

Nota: Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función Identificar. Fuente: Autoría propia.

Tabla A1.4

Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función proteger.

Proteger (PR): Se utilizan medidas de protección para gestionar los riesgos de seguridad cibernética de la organización.	Gestión de identidades, autenticación y control de acceso (PR.AA): El acceso a los activos físicos y lógicos se limita a los usuarios, servicios y hardware autorizados y se gestiona de forma proporcional al riesgo evaluado de acceso no autorizado.	PR.AA-01: La organización gestiona las identidades y credenciales de los usuarios, servicios y equipos autorizados.	La mayoría de las empresas tienen doble factor de autenticación.	Nivel 2 Riesgo informado
		PR.AA-02: Las identidades están comprobadas y vinculadas a credenciales basadas en el contexto de las interacciones.	No existe evidencias.	Nivel 1 Parcial
		PR.AA-03: Los usuarios, servicios y hardware están autenticados.	La mayoría de las empresas tienen doble factor de autenticación.	Nivel 2 Riesgo informado
		PR.AA-04: Las afirmaciones de identidad se protegen, transmiten y verifican.	No existe evidencias.	Nivel 1 Parcial
		PR.AA-05: Los permisos de acceso, los derechos y las autorizaciones se definen en una política, se gestionan, se aplican y se revisan, e incorporan los principios de privilegio mínimo y separación de funciones.	No existe evidencias.	Nivel 1 Parcial
		PR.AA-06: El acceso físico a los activos se gestiona, supervisa y aplica de forma proporcional al riesgo.	No existe evidencias.	Nivel 1 Parcial
	Concienciación y capacitación (PR.AT): Se proporciona al personal de la organización concienciación y capacitación en seguridad cibernética para que puedan realizar sus tareas relacionadas con la seguridad cibernética.	PR.AT-01: Se sensibiliza y capacita al personal para que disponga de los conocimientos y habilidades necesarios para realizar tareas penales teniendo en cuenta los riesgos de seguridad cibernética.	No se realiza, no existe evidencia.	Nivel 1 Parcial
		PR.AT-02: Se sensibiliza y capacita a las personas que desempeñan funciones especializadas para que posean los conocimientos y actitudes necesarios para realizar los tareas pertinentes teniendo en cuenta los riesgos de seguridad cibernética.	No se realiza, no existe evidencia.	Nivel 1 Parcial
	Seguridad de datos (PR.DS): Los datos se gestionan de forma coherente con la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	PR.DS-01: La confidencialidad, la integridad y la disponibilidad de los datos en reposo están protegidos.	No existe evidencias.	Nivel 1 Parcial
		PR.DS-02: La confidencialidad, la integridad y la disponibilidad de los datos en tránsito están protegidos.	No existe evidencias.	Nivel 1 Parcial
		PR.DS-10: La confidencialidad, la integridad y la disponibilidad de los datos en uso están protegidos.	No existe evidencias.	Nivel 1 Parcial
		PR.DS-11: Se crean, protegen, mantienen y comprueban copias de seguridad de los datos.	Se crean las copias de seguridad pero no se comprueban.	Nivel 1 Parcial
	Seguridad de plataformas (PR.PS): El hardware, el software (p. ej., firmware, sistemas operativos, aplicaciones) y los servicios de las plataformas físicas y virtuales se gestionan de acuerdo con la estrategia de riesgo de la organización para proteger su confidencialidad, integridad y disponibilidad.	PR.PS-01: Se establecen y aplican prácticas de gestión de la configuración.	No existe evidencias.	Nivel 1 Parcial
		PR.PS-02: Se mantiene, sustituye y elimina el software en función del riesgo.	No existe evidencias.	Nivel 1 Parcial
		PR.PS-03: Se mantiene, sustituye y elimina el hardware en función del riesgo.	No existe evidencias.	Nivel 1 Parcial
		PR.PS-04: Se generan registros y se ponen a disposición para una supervisión continua.	No existe evidencias.	Nivel 1 Parcial
		PR.PS-05: Se impide la instalación y la ejecución de software no autorizado.	No existe evidencias.	Nivel 1 Parcial
	Resiliencia de la infraestructura tecnológica (PR.IT): Las arquitecturas de seguridad se gestionan con la estrategia de riesgo de la organización a fin de proteger la confidencialidad, la integridad y la disponibilidad de los activos, así como la resiliencia de la organización.	PR.IT-01: Las redes y los sistemas están protegidos contra el acceso lógico y el uso no autorizados.	La mayoría de las empresas tienen redes, no existe evidencia de la protección.	Nivel 1 Parcial
		PR.IT-02: Los activos tecnológicos de la organización están protegidos de las amenazas del entorno.	No existe evidencias.	Nivel 1 Parcial
		PR.IT-03: Se implementan mecanismos para lograr los requisitos de resiliencia en situaciones normales y adversas.	No existe evidencias.	Nivel 1 Parcial
		PR.IT-04: Se mantiene una capacidad de recursos adecuada para garantizar la disponibilidad.	No existe evidencias.	Nivel 1 Parcial

Nota: Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF (ver Anexo Nro. 3). Función Proteger. Fuente: Autoría propia.

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica.

Tabla A1.5

Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función Detectar.

Detectar (DE): Se detectan y analizan posibles ataques y situaciones comprometedoras en materia de seguridad cibernética.	Monitoreo continuo (DECM): Los activos se monitorean para encontrar anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos	DE.CM-01: Las redes y los servicios de red se monitorean para detectar acontecimientos potencialmente adversos	Las mayoría de las empresas tienen redes, no existe evidencia del monitoreo	Nivel 1 Parcial
		DE.CM-02: Se monitorea el entorno físico para detectar posibles acontecimientos adversos	No existe evidencias	Nivel 1 Parcial
		DE.CM-03: Se monitorea la actividad del personal y el uso de la tecnología para detectar posibles acontecimientos adversos	No existe evidencias	Nivel 1 Parcial
		DE.CM-06: Se monitorean las actividades y los servicios de los proveedores de servicios externos para detectar acontecimientos potencialmente adversos.	No existe evidencias	Nivel 1 Parcial
		DE.CM-09: Se monitorean el hardware y el software informáticos, los entornos de ejecución y sus datos para detectar posibles acontecimientos adversos	Algunas empresas realizan el monitoreo pero no existe evidencia	Nivel 1 Parcial
	Análisis de eventos adversos (DEAE): Se analizan anomalías, indicadores de compromiso y otros acontecimientos potencialmente adversos para caracterizarlos y detectar incidentes de seguridad cibernética	DE.AE-02: Los acontecimientos potencialmente adversos se analizan para comprender mejor las actividades asociadas	No existe evidencias	Nivel 1 Parcial
		DE.AE-03: Se correlaciona la información procedente de diversas fuentes	No existe evidencias	Nivel 1 Parcial
		DE.AE-04: Se comprende el impacto estimado y el alcance de los acontecimientos adversos	No existe evidencias	Nivel 1 Parcial
		DE.AE-06: La información sobre acontecimientos adversos se proporciona al personal y a las herramientas autorizadas	No existe evidencias	Nivel 1 Parcial
		DE.AE-07: La inteligencia sobre amenazas cibernéticas y otra información contextual se integran en el análisis	No existe evidencias	Nivel 1 Parcial
		DE.AE-08: Se declaran incidentes cuando los acontecimientos adversos cumplen con los criterios de incidente definidos	No existe evidencias	Nivel 1 Parcial

Nota: Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF (ver Anexo Nro. 3). Función Detectar. Fuente: Autoría propia.

Tabla A1.6

Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función Responder.

Responder (RS): Se toman medidas en relación con un incidente de seguridad cibernética detectado	Gestión de incidentes (RS.MA): Se gestionan las respuestas a los incidentes de seguridad cibernética detectados	RS.MA-01: Se ejecuta el plan de respuesta a incidentes en coordinación con los terceros pertinentes una vez que se declara un incidente	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.MA-02: Se clasifican y validan los informes de incidentes	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.MA-03: Se clasifican y priorizan los incidentes	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.MA-04: Se escalan o elevan los incidentes según sea necesario	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.MA-05: Se aplican los criterios para iniciar la recuperación de incidentes	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
	Análisis de incidentes (RS.AN): Se llevan a cabo investigaciones con el fin de garantizar una respuesta eficaz y apoyar las actividades forenses y de recuperación	RS.AN-03: Se realizan análisis para determinar lo que ocurrió durante un incidente y la causa raíz del mismo	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.AN-06: Se registran las acciones realizadas durante una investigación y se preservan la integridad y la procedencia de los registros	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.AN-07: Se recopilan los datos y metadatos del incidente y se preservan su integridad y su procedencia	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.AN-08: Se estima y valida la magnitud de un incidente.	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
	Notificación y comunicación de la respuesta al incidente (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas, según lo exijan las leyes, las normativas o las políticas	RS.CO-02: Se notifican los incidentes a las partes interesadas internas y externas	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.CO-03: La información se comparte con las partes interesadas internas y externas designadas	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
	Mitigación de incidentes (RS.MI): Se llevan a cabo actividades a fin de evitar la expansión de un incidente y mitigar sus efectos	RS.MI-01: Se contienen los incidentes	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial
		RS.MI-02: Se erradican los incidentes	No existe evidencia de actividades de respuesta a incidentes	Nivel 1 Parcial

Nota: Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF(ver Anexo Nro. 3). Función Responder. Fuente: Autoría propia.

Tabla A1.7

Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF. Función Recuperar.

Recuperar (RC): Se restauran los activos y las operaciones afectados por un incidente de seguridad cibernética	Ejecución del Plan de Recuperación de Incidentes (RC.RP): Se realizan actividades de restauración que garantizan la disponibilidad operativa de los sistemas y servicios afectados por incidentes de seguridad cibernética	RC.RP-01: La parte de recuperación del plan de respuesta a incidentes se ejecuta una vez que se inicia desde el proceso de respuesta a incidentes	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
		RC.RP-02: Se seleccionan, delimitan, priorizan y llevan a cabo las acciones de recuperación	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
		RC.RP-03: Se verifica la integridad de las copias de seguridad y otros activos de restauración antes de usarlos para la restauración	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
		RC.RP-04: Se tienen en cuenta las funciones críticas de la misión y la gestión de riesgos de seguridad cibernética para establecer normas operativas posteriores al incidente	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
		RC.RP-05: Se verifica la integridad de los activos restaurados, se restauran los sistemas y servicios y se confirma el estado operativo normal	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
		RC.RP-06: Se declara el fin de la recuperación del incidente sobre la base de criterios y se completa la documentación relacionada con el incidente	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
	Comunicación de la recuperación del incidente (RC.CO): Se coordinan las actividades de restauración con las partes internas y externas	RC.CO-03: Las actividades de recuperación y los progresos en el restablecimiento de las capacidades operativas se comunican a las partes interesadas internas y externas designadas	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial
		RC.CO-04: Las actualizaciones públicas sobre la recuperación del incidente se comporten mediante el uso de métodos y mensajes aprobados	No existe evidencia de actividades de recuperación de incidentes	Nivel 1 Parcial

Nota importante: Para efectos de Autodiagnóstico, en esta tesis de maestría, solo se diligencio la primera parte de este formato denominada PERFIL ACTUAL.

Nota: Autodiagnóstico del sector flexográfico según el marco NIST 2.0 CSF (ver Anexo Nro. 3). Función Recuperar. Fuente: Autoría propia.

Debe anotarse, que el presente autodiagnóstico, al igual que en el caso anterior, tiene o consta de dos (2) etapas, una primera etapa que evalúa el estado actual y una segunda etapa que evalúa el estado de la infraestructura o sistema informático una vez implementados los respectivos controles. Esta segunda parte del autodiagnóstico se efectuará en la fase 3 de verificación o validación del modelo de esta tesis de maestría, para asegurar el mejoramiento del sistema computacional y la mitigación del riesgo informático.

De otra parte, la realización de estos autodiagnósticos, tanto en su versión acorde con el marco NIST 2.0 CSG y en su versión según la norma ISO 27001, tuvieron el objetivo de identificar brechas de seguridad y oportunidades de mejoramiento y, adicionalmente, sirvieron como insumo para la posterior evaluación y análisis del riesgo informático, consolidados, más adelante en esta tesis de maestría, mediante la elaboración de la correspondiente matriz de riesgo informático y su respectivo mapa de calor.

La realización de este par de autodiagnósticos tuvo el objetivo de identificar brechas y oportunidades de mejora y, adicionalmente, sirvió como insumo para la posterior evaluación y análisis de riesgos informáticos, consolidada mediante la elaboración de un mapa de calor o matriz de riesgo informático. La convergencia en los resultados de

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica.

ambas autoevaluaciones confirma la realidad del estado de la seguridad de la información en la infraestructura computacional asociada a la gestión de la cadena de producción del sector flexográfico, sus necesidades y requerimientos y conforma un insumo primordial para la siguiente actividad (Actividad 1.2. Estructuración de una matriz de riesgo informático y mapa de calor con sus respectivos controles).

Nota Importante:

Para mayor detalle sobre las autoevaluaciones obtenidas con base en los resultados de la encuesta, por favor, ver Anexo Nro. 3 (Excel).

Anexo Nro. 3

Autodiagnósticos obtenidos de los resultados de la encuesta de diagnóstico sectorial flexográfico (Autoevaluaciones según norma ISO 27001 y marco NIST 2.0 CSF)

Ver archivo Excel (Anexo Nro. 3 - .xlsx)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 1 - Actividad 1.2

Anexo Nro. 4

Matriz de riesgo informático y mapa de calor - Análisis y evaluación del riesgo cibernético del sector flexográfico

Ver archivo Excel (Anexo Nro. 4 - .xlsx)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 1 - Actividad 1.2 - ENTREGABLE

Anexo Nro. 5

Controles seleccionados de la revisión de estándares internacionales y buenas prácticas de seguridad informática para el sector flexográfico

Ver archivo Excel (Anexo Nro. 5 - .xlsx)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 2 - Actividad 2.1 - ENTREGABLE

Anexo Nro. 6

Modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 2 - Actividad 2.2 - ENTREGABLE

Anexo Nro. 6

Modelo de ciberseguridad para la industria flexográfica

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 2 - ACTIVIDAD 2.1 - ENTREGABLE

MODELO DE CIBERSEGURIDAD PARA EL SECTOR FLEXOGRÁFICO



Anexo Nro. 6

Desglose detallado y descripción de subactividades del modelo de ciberseguridad para la industria flexográfica

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 2 - ACTIVIDAD 2.1 - ENTREGABLE

DESGLOSE DE LAS SUBACTIVIDADES DEL MODELO DE CIBERSEGURIDAD PARA EL SECTOR FLEXOGRÁFICO



Anexo Nro. 7

Validación del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 3 - Actividad 3.1 - ENTREGABLE

I.T.M.

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Ing. Edgar Alberto Acevedoarango e Ing. Adriana María Echeverri Londoño

VALIDACIÓN DEL MODELO DE CIBERSEGURIDAD PARA LA INFRAESTRUCTURA INFORMÁTICA ASOCIADA A LA CADENA DE PRODUCCIÓN DEL SECTOR FLEXOGRÁFICO

ENCUESTA FINAL PARA TESIS DE MAESTRÍA

Sección 1 - CONSENTIMIENTO INFORMADO

Con el fin de realizar la validación de una propuesta de modelo de ciberseguridad desarrollado en el marco de la Maestría en Seguridad Informática del ITM, el cual busca la protección de la infraestructura informática asociada a la cadena productiva de las PYME ante eventos o ataques cibernéticos que puedan afectar las empresas de la industria flexográfica, le solicitamos su amable y apreciada participación en esta encuesta, que pretende verificar cómo dicho modelo de ciberseguridad puede proteger la confidencialidad, integridad y disponibilidad de la seguridad de la información del sector flexográfico.

Los ciberataques son un cierto tipo de incidentes informáticos maliciosos que pueden llegar a impactar gravemente a una compañía y, en particular, a su línea productiva. Es importante resaltar que las respuestas a la encuesta serán tratadas de manera confidencial y anónima, y solo se usarán exclusivamente para efectos académicos y de investigación, y cuyos resultados solo se expondrán análisis finales y conclusiones de la evaluación del modelo de ciberseguridad propuesto.

Con respecto a posible información personal o empresarial, la encuesta será manejada con estricta ética, legalidad y confidencialidad, conforme a lo establecido en la Ley 1581 de 2012 y el Decreto 1377 de 2013, que regulan la protección de datos personales y tratamiento de información sensible en Colombia. En consecuencia, los datos recabados serán utilizados exclusivamente para los fines de estudio académico e investigativo manifestados y no serán compartidos con terceros ajenos a la investigación realizada. Del mismo modo, dichos datos sean almacenados de manera segura y se adoptarán las medidas necesarias para evitar su acceso no autorizado por parte de terceros. En todo momento, durante el desarrollo y consolidación de los datos de esta encuesta, usted y su institución, o compañía, tendrán derecho a consultar, actualizar, rectificar o suprimir sus datos personales o información sensible que considere, así como a revocar la autorización suministrada para su tratamiento y uso, conforme a los procedimientos establecidos en la legislación colombiana.

Si está de acuerdo en participar y responder a esta encuesta, por favor marque "Sí"; de lo contrario, marque "No".

Si ____ No ____

Sección 2 – ESCALA DE LIKERT PARA OPCIONES DE RESPUESTA

A continuación, se presentan las diversas opciones de respuesta a las preguntas de la encuesta, acorde a la escala de Likert:

ESCALA DE LIKERT DE RESPUESTAS DE LA ENCUESTA DE VALIDACIÓN DEL MODELO DE CIBERSEGURIDAD.					
Escala de Valores		Respuestas posibles			
Letras	Números				
Cinco	5	Supremamente efectivo y eficaz	El modelo de ciberseguridad es idóneo y no requiere ajustarse.	Muy Alto	Total y completamente de acuerdo
Cuatro	4	Muy efectivo y eficaz	El modelo de ciberseguridad tiene una implementación de ciberseguridad muy buena y suficiente y no requiere ajustarse.	Alto	Muy de acuerdo
Tres	3	Efectivo y eficaz	El modelo de ciberseguridad tiene buenas funcionalidades que brindan seguridad y no requiere de ajuste fino de sus funciones.	Medio - Alto	De acuerdo
Dos	2	Medianamente efectivo y medianamente eficaz	El modelo de ciberseguridad tiene implementación muy básica que, logra brindar la protección necesaria, pero, no completa, por lo que requiere del ajuste fino de algunas pocas funciones específicas.	Moderado	Moderadamente de acuerdo
Uno	1	Aceptable	El modelo de ciberseguridad tiene una implementación de ciberseguridad limitada, pero, requiere del ajuste de algunas funciones.	Bajo	Poco de acuerdo
Cero	0	Requiere Ajuste	El modelo de ciberseguridad requiere un ajuste completo y significativo.	Muy Bajo	En desacuerdo

Nota: El valor Cinco (5) expresa un modelo de Ciberseguridad idóneo que no requiere ajuste alguno, mientras que el valor Cero (0) expresa que el prototipo cibernético de protección no es adecuado y requiere un ajuste completo y significativo. De otra parte, los valores intermedios expresan la gradualidad y granulosidad de la efectividad y de eficacia de la protección que brinda el modelo de ciberseguridad, ambos extremos y según el contexto de la pregunta. Fuente: Tomado de: Autoría propia.

Contactos:

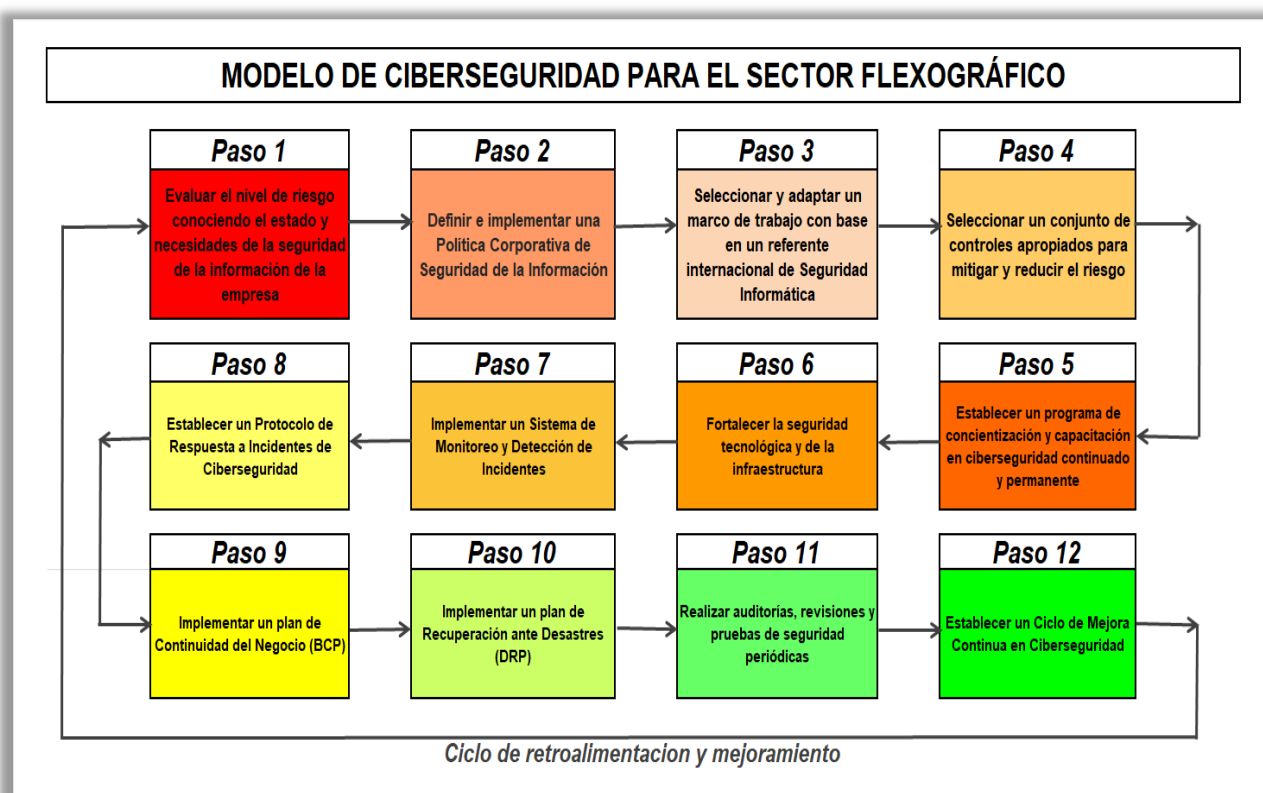
Para más información, dudas o inquietudes, los participantes pueden contactar a:

- Ing. **Edgar Alberto Acevedoarango:**
317 452 23 26 - edgaracevedoarango1131337@correo.itm.edu.co
- Ing. **Adriana María Echeverri Londoño.**
317 510 38 60 - adrianaecheverri1131341@correo.itm.edu.co

Sección 3 - ENCUESTA

El modelo de ciberseguridad esta basado en estándares internacionales y buenas prácticas, y permite conservar la confiabilidad, integridad y disponibilidad de los sistemas informáticos que puede verse afectada por evento de cibernéticos, generando posibles consecuencias negativas en las operaciones, equipos informáticos y/o servicios tecnológicos en los procesos productivos críticos de una PYME del sector flexográfico.

En la siguiente gráfica se presenta el modelo general:



A continuación, se presenta, en forma más detallada e incluidas las subactividades a desarrollar por cada uno de los pasos metodológicos propuestos, el modelo de ciberseguridad general, desarrollado en la tesis de grado para la protección de la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura informática asociada a la gestión de la cadena productiva crítica de la industria flexográfica:



Considerando el modelo de ciberseguridad anteriormente propuesto (con su respectivo detalle), por favor, marque con una equis (X) la respuesta que considere más apropiada y pertinente y un fiel reflejo de sus consideraciones sobre la efectividad y eficiencia del modelo de ciberseguridad propuesto para el aseguramiento de la información:

El modelo de ciberseguridad que le ha sido presentado, para la protección cibernética de la infraestructura informática y equipos computacionales de gestión y operación de su cadena de producción crítica:

1. *¿En qué nivel cree Ud. que contribuye a construir o mejorar sus estrategias o planes corporativos de seguridad informática y, en general, a mejorar la ciberseguridad?*

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

2. *Considerando, las recomendaciones sobre cómo implementar medidas y controles de seguridad ¿En qué nivel cree Ud. que su adopción contribuiría a la disminución del nivel de riesgo informático?*

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

3. *¿En qué nivel consideraría Ud. que, reforzar su personal de ciberseguridad, ayudaría a mitigar y reducir su nivel de riesgo ante ciberataques e incidentes informáticos?*

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

4. *¿En qué nivel implementaría Ud. los pasos que se recomiendan y que se sugieren, entre ellos mejorar los controles de acceso con contraseñas más seguras y el uso de doble factor de autenticación, incluyendo implementar los controles respectivos sugeridos, para mejorar la protección y disminuir el riesgo cibernético?*

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

5. *¿En qué nivel consideraría Ud. implementar programas permanentes y continuos de capacitación y actualización en ciberseguridad para todo su personal?*

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

6. ¿En qué nivel cree Ud. que, contar o fortalecer su sistema de respaldo y recuperación de información de producción (production backup), incluida copia en la nube sería conveniente y recomendable, para garantizar la continuidad operativa y la resiliencia de su cadena de producción crítica?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

7. ¿En qué nivel considera Ud. que, implementar de manera periódica el análisis y evaluación del riesgo informático con el fin de mitigar vulnerabilidades, sería una práctica de seguridad conveniente y recomendable para su empresa,?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

8. ¿En qué nivel considera Ud. que su adopción contribuiría a conseguir, o fomentar, el compromiso de la gerencia con la ciberseguridad, y a crear, o fortalecer, una cultura de seguridad informática al interior de su organización?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

9. ¿En qué nivel considera Ud. que los controles y medidas sugeridos son apropiados para la protección de sus redes internas/externas (incluido el acceso a Internet)?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

10. ¿En qué nivel considera Ud. que su adopción contribuiría a la reducción de impactos negativos ocasionados por ciberataques?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

11. ¿En qué nivel considera Ud. que su adopción contribuiría al mejoramiento de la gestión de atención y respuesta de incidentes informáticos?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

12. En general, ¿En qué nivel considera Ud. que el modelo de ciberseguridad propuesto protegerá la confidencialidad, integridad y disponibilidad de la seguridad de la información de su cadena de producción crítica?

0 ____ 1 ____ 2 ____ 3 ____ 4 ____ 5 ____

Anexo Nro. 8

Tabulación de resultados de encuesta de validación de modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico

Ver archivos Excel (Anexo Nro. 8 - .xlsx)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 3 - Actividad 3.2 - ENTREGABLE

Tabulación y análisis de resultados de la encuesta de validación final del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico.

Resultados obtenidos y análisis estadístico de la encuesta de “Validación del modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción del sector flexográfico”

A continuación, se consignan los resultados obtenidos y su respectivo análisis estadístico y conceptual. También, se consignan las autoevaluaciones derivadas que servirán de insumo para la elaboración del análisis y evaluación de riesgo final, es decir, con el modelo de ciberseguridad propuesto, mediante la construcción de la respectiva matriz de riesgo y su mapa de calor.

Pregunta 1. *¿En qué nivel cree Ud. que contribuye a construir o mejorar sus estrategias o planes corporativos de seguridad informática y, en general, a mejorar la ciberseguridad?*

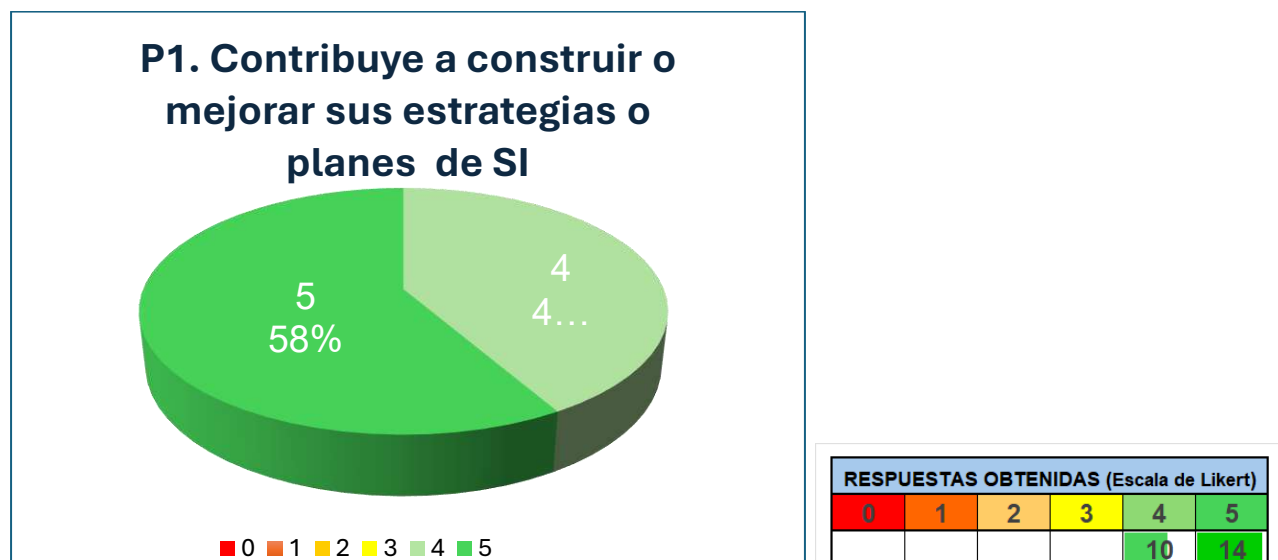


Fig. A8.1

Resultados obtenidos en la primera pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la primera pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Como bien se aprecia, a partir de los resultados mostrados en la figura anterior, se evidencia que, la mayoría de las organizaciones del sector flexográfico encuestadas (el 100% de las respuestas concentradas entre los niveles 4 y 5 de la escala de Likert) perciben que el modelo de ciberseguridad propuesto ayuda y contribuye de manera significativa a fortalecer o construir sus estrategias y planes de seguridad informática. Este hallazgo revela que el prototipo cibernético protectivo no solo ha sido bien acogido, sino que, también, es bien valorado en aras a su potencial adopción como un instrumento que aporta claridad, coherencia y estructura a la gestión de riesgos digitales en las PYMEs del sector.

De otra parte, la positividad de la percepción reflejada en los resultados indica un avance relevante en la madurez organizacional en materia de ciberseguridad, pues las empresas consideran que el modelo de ciberseguridad propuesto les permite alinearse con buenas prácticas internacionales, mejorar la protección de su infraestructura crítica y disponer de un marco capaz de orientar sus decisiones para asegurar la continuidad operativa y contribuir a la reducción de vulnerabilidades asociadas a la infraestructura IT asociada a sus procesos productivos esenciales.

Pregunta 2. Considerando, las recomendaciones sobre cómo implementar medidas y controles de seguridad ¿En qué nivel cree Ud. que su adopción contribuiría a la disminución del nivel de riesgo informático?

Como se puede apreciar en los resultados obtenidos y mostrados en la figura siguiente, la totalidad de los encuestados valora de manera altamente positiva el impacto que tendría la adopción del modelo de ciberseguridad propuesto; especialmente, en cuanto a la disminución del nivel de riesgo informático. Con un 46% ubicado en el nivel 4 y un 54% en el nivel 5 de la escala de Likert, se evidencia que, las organizaciones del sector flexográfico perciben que la implementación de los controles, medidas y recomendaciones del prototipo cibernético protectivo contribuiría de forma sustancial y significativa, a mitigar ciberamenazas, reducir vulnerabilidades, mitigar la exposición al riesgo y fortalecer la postura de seguridad de sus sistemas, procesos e infraestructura IT asociada a sus procesos productivos críticos.

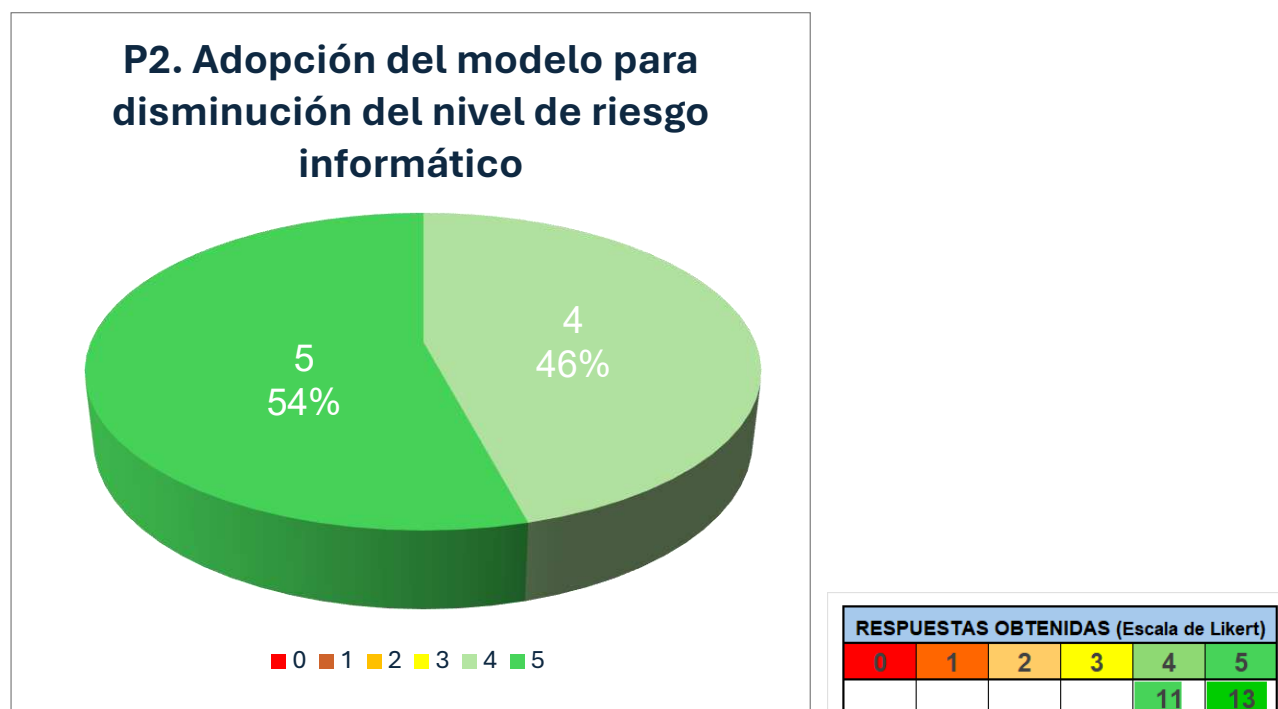


Fig. A8.2

Resultados obtenidos en la segunda pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la segunda pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

De otro lado, esta apreciación confirma, de manera generalizada, que, el modelo de ciberseguridad diseñado no solo es pertinente, sino que, también, es considerado como un mecanismo eficaz y efectivo para incrementar la resiliencia digital de las PYMEs del sector.

Adicionalmente, la clara inclinación en las respuestas obtenidas hacia los niveles superiores de la escala indica que las empresas reconocen el valor estratégico de contar con lineamientos estructurados y estandarizados para la gestión del riesgo informático. En consecuencia, estos resultados refuerzan la necesidad, relevancia e importancia que asignan las empresas a su capacidad para responder adecuadamente a las brechas de ciberseguridad identificadas y ofrecen una ruta práctica para elevar el nivel de seguridad y continuidad operativa en la industria flexográfica.

Pregunta 3. ¿En qué nivel consideraría Ud. que, reforzar su personal de ciberseguridad, ayudaría a mitigar y reducir su nivel de riesgo ante ciberataques e incidentes informáticos?

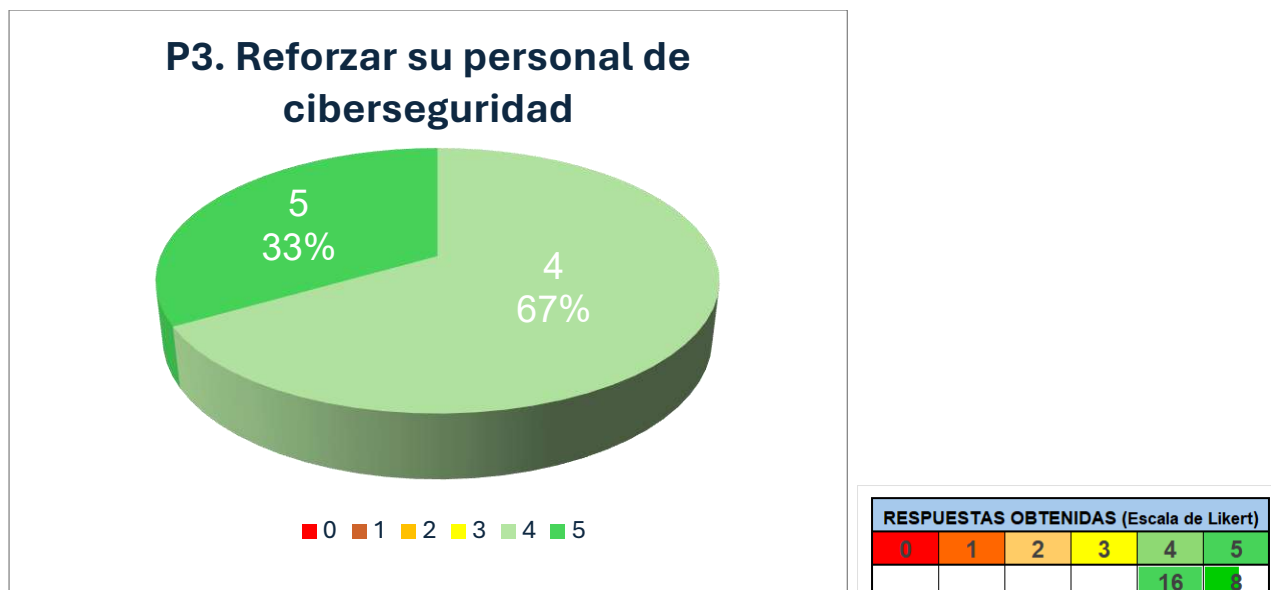


Fig. A8.3

Resultados obtenidos en la tercera pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la tercera pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

La figura anterior, en la cual se consignan los resultados obtenidos, evidencia que las organizaciones del sector flexográfico consideran altamente relevante el fortalecimiento de su personal de ciberseguridad como un factor especialmente significativo en la estrategia para mitigar el riesgo ante ciberataques e incidentes informáticos, pues, con un 67% de respuestas en el nivel 4 y un 33% en el nivel 5, se decanta que la totalidad de las organizaciones encuestadas percibe que aumentar las capacidades, competencias y cantidad de personal especializado en seguridad informática tendría un impacto directo y sustancial en la reducción de su exposición a amenazas digitales.

De esta manera se concluye que la concentración, de las respuestas obtenidas, en los niveles superiores de la escala de Likert, demuestran que la industria reconoce la importancia del talento humano como un componente esencial dentro de cualquier modelo de ciberseguridad. Adicionalmente, la valoración obtenida confirma que la disponibilidad de personal capacitado no solo permite una mejor implementación de controles y medidas técnicas, sino que contribuye a fortalecer la vigilancia continua, la respuesta ante incidentes y la resiliencia operativa. De esta manera, los resultados de la encuesta de validación respaldan la pertinencia del modelo propuesto, reafirmando la necesidad de integrar estrategias orientadas al desarrollo de

capacidades humanas como parte fundamental de la protección de la infraestructura IT asociada a la cadena de producción crítica del sector flexográfico.

Pregunta 4. ¿En qué nivel implementaría Ud. los pasos que se recomiendan y que se sugieren, entre ellos mejorar los controles de acceso con contraseñas más seguras y el uso de doble factor de autenticación, incluyendo implementar los controles respectivos sugeridos, para mejorar la protección y disminuir el riesgo cibernético?

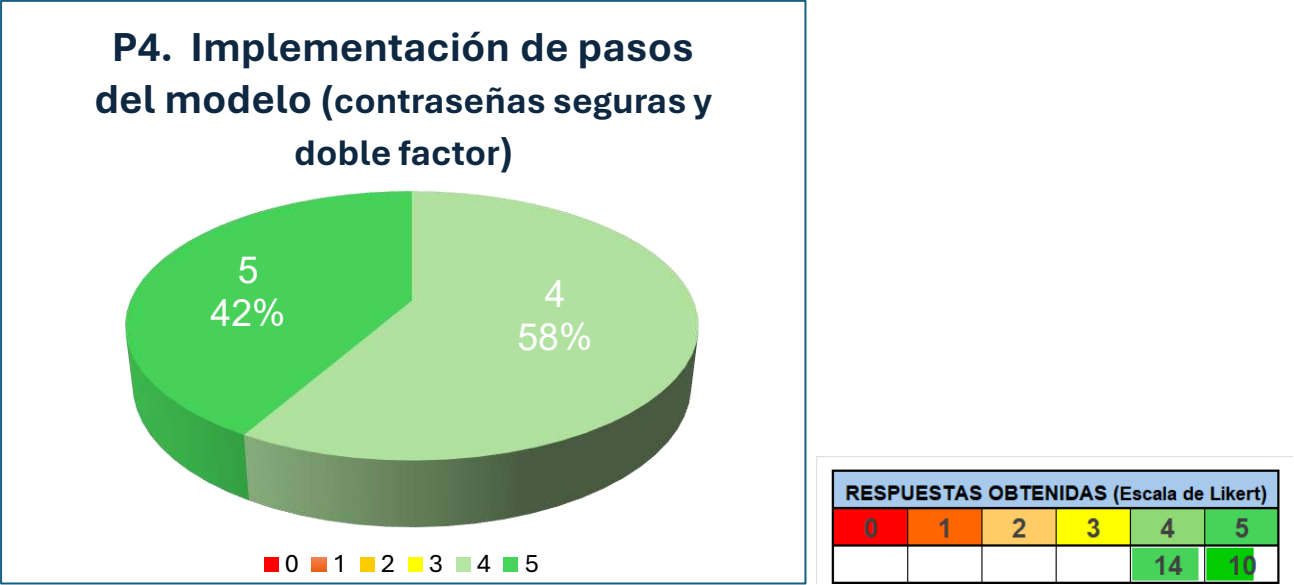


Fig. A8.4

Resultados obtenidos en la cuarta pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la cuarta pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Los resultados, consignados en la figura anterior, evidencian una alta disposición por parte de las organizaciones de la industria en estudio para implementar los pasos y controles recomendados por el modelo de ciberseguridad propuesto, especialmente aquellos relacionados con el fortalecimiento de los mecanismos de acceso, como el uso de contraseñas seguras y la autenticación de doble factor. Con un 58% de las respuestas en el nivel 4 y un 42% en el nivel 5, se observa que la totalidad de los encuestados percibe que estas medidas tendrían un impacto tan inmediato como significativo en la mejora de la protección de sus sistemas y en la reducción del riesgo cibernético asociado a accesos no autorizados.

De hecho, la marcada concentración de las respuestas obtenidas en los niveles superiores de la escala de Likert, reflejan una clara conciencia sobre la importancia de adoptar controles esenciales y de rápida implementación, los cuales forman parte fundamental de las mejores prácticas internacionales de ciberseguridad. Asimismo, los resultados obtenidos respaldan la pertinencia del prototipo cibernético protectivo diseñado y propuesto al demostrar, que las empresas consideran viable y necesaria la adopción de estas medidas para fortalecer su postura de seguridad. En conjunto, estos hallazgos reafirman que las recomendaciones planteadas en el modelo de ciberseguridad desarrollado responden directamente a necesidades de seguridad informática críticas del sector y ofrecen soluciones prácticas orientadas a la mitigación efectiva del riesgo informático.

Pregunta 5. ¿En qué nivel consideraría Ud. implementar programas permanentes y continuos de capacitación y actualización en ciberseguridad para todo su personal?



Fig. A8.5

Resultados obtenidos en la quinta pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la quinta pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

La información contenida en el gráfico anterior, derivada de los resultados de la encuesta de validación final del modelo de ciberseguridad, revela unan aceptación mayoritaria y robusta, de la necesidad de implementar medidas de formación continua en ciberseguridad al interior de las organizaciones, lo cual valida el componente de capacitación y concientización que propone el

prototipo cibernético protector para la industria flexográfica. De hecho, con un 58% de las respuestas ubicadas en el nivel 5 (de máxima prioridad) y el 42% restante en el nivel 4 (prioridad alta), el 100% de los participantes de la encuesta manifiesta una intención de adopción elevada de la práctica de la capacitación continua.

En efecto, los resultados reflejan una distribución que evidencia que el sector en estudio reconoce que establecer programas sistemáticos y permanentes de formación, entrenamiento y actualización es uno de los factores clave en una estrategia de seguridad informática cuyo propósito sea elevar la protección de la infraestructura IT asociada a la gestión de la cadena de producción crítica sectorial. En este sentido, es claro que estas iniciativas se perciben no como un gasto, sino, más bien, como una inversión esencial con un retorno inmediato en la reducción de vulnerabilidades asociadas al error humano, tales como el éxito de ataques de ingeniería social, lo cual, a la larga, conlleva a la mitigación del nivel de riesgo cibernético en las empresas y, especialmente, en las PYMEs.

Adicionalmente, nótese que los resultados obtenidos dotan de gran solidez al componente humano dentro del prototipo cibernético propuesto, pues, al confirmar que las organizaciones están dispuestas a comprometerse con la educación en ciberseguridad, se verifica que el modelo de ciberseguridad diseñado aborda una preocupación clave del sector y propone una solución considerada, tanto necesaria, como factible pues la valoración de dichos resultados consolidan la premisa de que la ciberseguridad en la industria flexográfica debe construirse sobre una base de personal consciente y capacitado. Este hallazgo reafirma la idoneidad y la pertinencia práctica del modelo de ciberseguridad desarrollado, demostrando su capacidad para ofrecer respuestas efectivas a las demandas reales de la mitigación de riesgos informáticos, particularmente, en cuanto a la confidencialidad, integridad y disponibilidad de la seguridad de la información.

Pregunta 6. ¿En qué nivel cree Ud. que, contar o fortalecer su sistema de respaldo y recuperación de información de producción (production backup), incluida copia en la nube sería conveniente y recomendable, para garantizar la continuidad operativa y la resiliencia de su cadena de producción crítica?

Los resultados consignados en la figura siguiente y obtenidos de la aplicación del instrumento, evidencian una aceptación mayoritaria (100% de las respuestas concentradas entre los niveles 4 y 5 de la escala de Likert) por parte de las organizaciones y, en particular, de las PYMEs, de la

industria flexográfica para fortalecer los sistemas de respaldo y recuperación de información (backups) como un componente esencial para la protección de la seguridad de la información con el modelo de ciberseguridad propuesto. En general, el sector ve las copias de seguridad como un factor clave en su seguridad y de suprema utilidad para lograr la recuperación de los sistemas IT en caso de ciberataque o falla tecnológica.

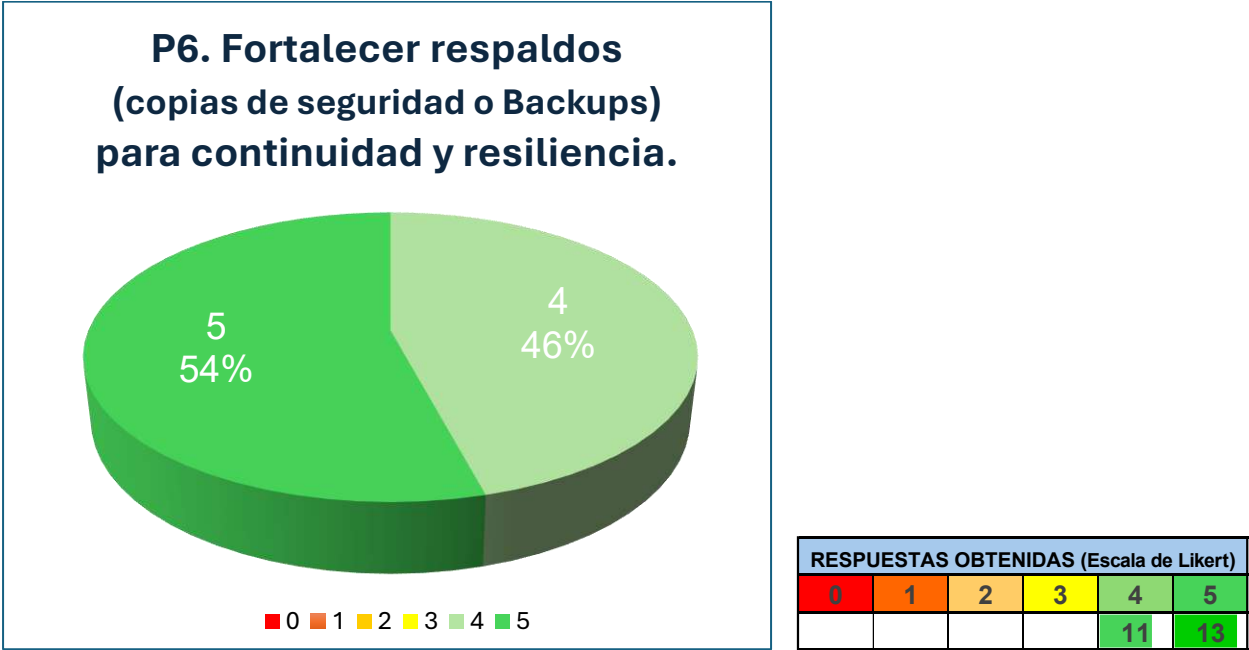


Fig. A8.6

Resultados obtenidos en la sexta pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la sexta pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

En efecto, con un 54% de las respuestas ubicadas en el nivel 5 y el 46% restante en el nivel 4, los encuestados manifiestan que la implementación de estrategias robustas de backup, incluyendo soluciones en la nube, es vital para garantizar la continuidad operativa y la resiliencia frente a ciberincidentes. Notese que, esta distribución refleja una clara conciencia sectorial respecto a que un sistema de respaldo eficiente es la última línea de defensa contra las ciberamenazas, particularmente, para ciberataques con ransomware, o contra fallas tecnológicas, calamidades o desastres de cualquier naturaleza, siendo las copias de seguridad elementos fundamentales para la rápida recuperación de la infraestructura IT asociada a la cadena de producción crítica.

En conjunto, los resultados obtenidos reafirman que las recomendaciones planteadas están perfectamente alineadas con las mejores prácticas internacionales de resiliencia cibernética (como la regla 3-2-1 de backup) y ofrecen una solución práctica, viable y altamente valorada, por el sector en estudio, para la mitigación efectiva del riesgo y sus impactos, ante la eventual ocurrencia de un ciberataque.

Pregunta 7. ¿En qué nivel considera Ud. que, implementar de manera periódica el análisis y evaluación del riesgo informático con el fin de mitigar vulnerabilidades, sería una práctica de seguridad conveniente y recomendable para su empresa?

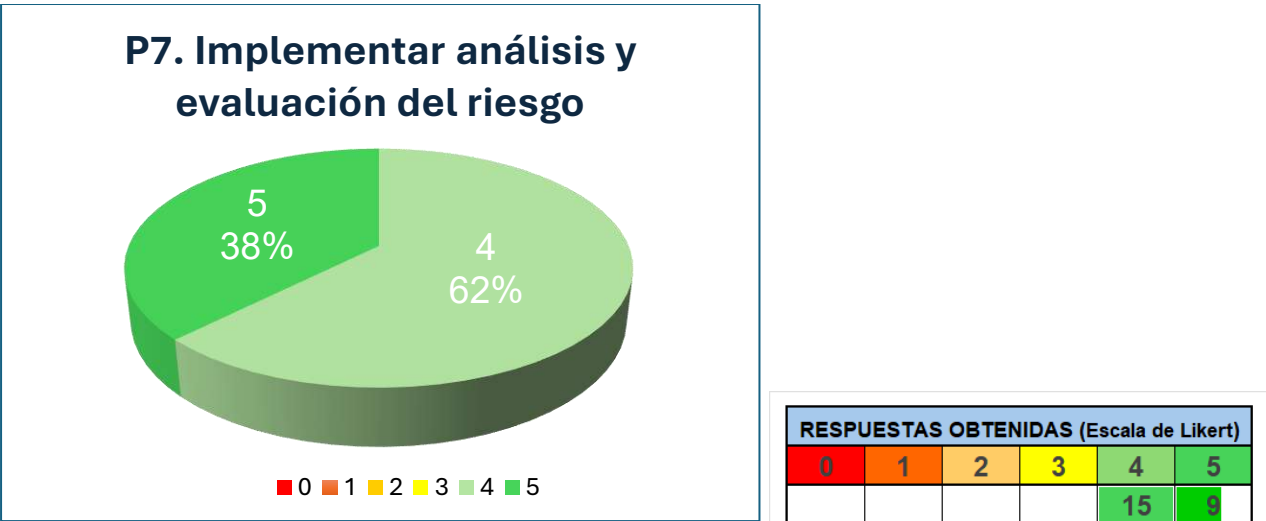


Fig. A8.7

Resultados obtenidos en la séptima pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la séptima pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Los hallazgos encontrados, y que se presentan en la figura anterior, evidencian una voluntad mayoritaria (100% de las respuestas concentradas entre los niveles 4 y 5) por parte de las organizaciones de la industria flexográfica para implementar el análisis y evaluación del riesgo informático como una práctica de seguridad necesaria a realizar de manera continua y periódica, pues, con un 62% de las respuestas ubicadas en el nivel 4 y un 38% en el nivel 5, los encuestados demuestran que la gestión proactiva de riesgos es vista como una práctica de seguridad, además de necesaria, como conveniente y recomendable. Esta distribución de resultados tan favorable indica que el sector en estudio ha trascendido la seguridad reactiva,

reconociendo el valor de identificar, medir y priorizar vulnerabilidades para mitigar el riesgo cibernético antes de que se materialice un incidente.

En este consenso, la mayoría de las empresas, validan en los niveles superiores y de forma contundente la inclusión de la gestión de riesgos, como elemento preponderante del modelo de ciberseguridad propuesto, pues, al confirmar que consideran la evaluación continua del riesgo como una medida esencial, se corrobora que el modelo está alineado con la necesidad de establecer un marco de seguridad maduro basado en información en tiempo real sobre el nivel de riesgo y superficie de exposición al mismo. En conjunto, los resultados obtenidos reafirman que las recomendaciones planteadas en esta área no solo responden a las mejores prácticas de gobernanza de ciberseguridad, sino que, también, el prototipo cibernético protectivo propuesto ofrece una solución estratégica que es percibida como práctica y necesaria por el sector para orientar las inversiones en soluciones tecnológicas y los esfuerzos de seguridad hacia las áreas prioritarias, críticas o de mayor impacto.

Pregunta 8. ¿En qué nivel considera Ud. que su adopción contribuiría a conseguir, o fomentar, el compromiso de la gerencia con la ciberseguridad, y a crear, o fortalecer, una cultura de seguridad informática al interior de su organización?

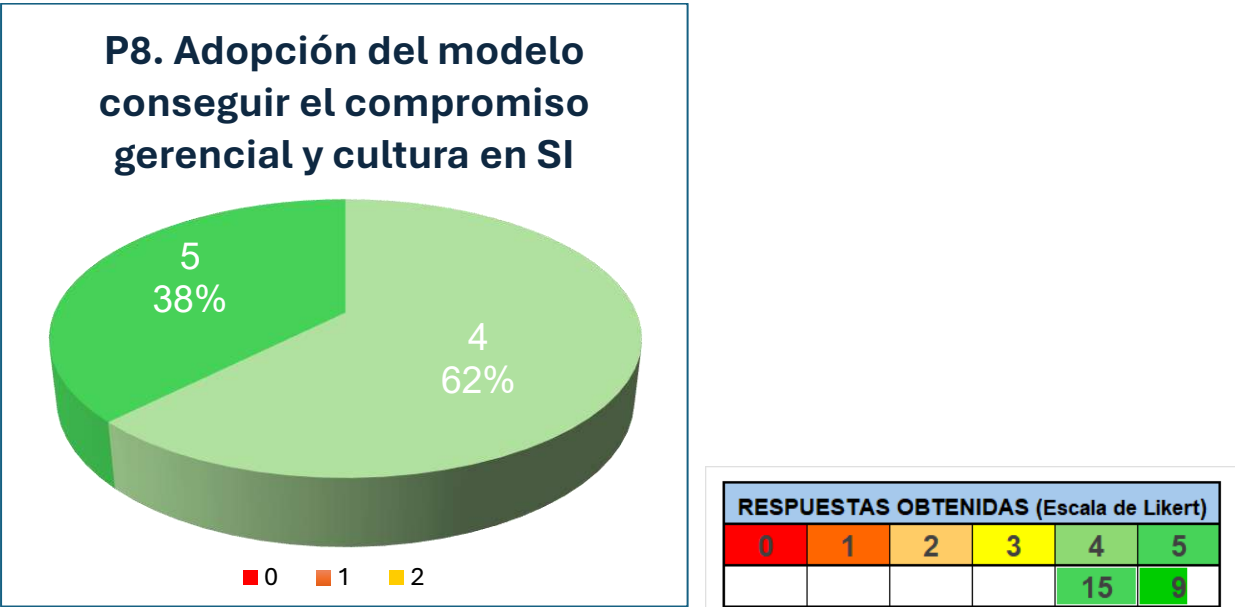


Fig. A8.8

Resultados obtenidos en la octava pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la octava pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

La figura anterior presenta los resultados obtenidos (100% de las respuestas concentradas entre los niveles 4 y 5), los cuales, revelan una expectativa extremadamente alta por parte de la industria flexográfica en cuanto al impacto transformador del modelo de ciberseguridad propuesto en la gobernanza y la cultura organizacional. En efecto, con un 62% de las respuestas ubicadas en el nivel 4 y un 38% en el nivel 5, los encuestados perciben que, la adopción del prototipo cibernético protectivo desarrollado, no solo mejorará los controles técnicos, sino que, también, actuará como un catalizador para obtener el compromiso gerencial y para crear o fortalecer una cultura de seguridad informática al interior de cada organización.

La gráfica indica que los líderes sectoriales valoran y ven el modelo de ciberseguridad propuesto como una herramienta clave para formalizar la ciberseguridad, elevándola al nivel de decisión estratégica. En este contexto, se valida la capacidad integral y el alcance estratégico del modelo de ciberseguridad desarrollado, pues, los hallazgos confirman que las empresas consideran que, la adopción de este facilitará la alineación entre la estrategia de negocio, la continuidad y resiliencia operacionales, así, como también, con respecto a la seguridad informática.

En efecto, los resultados corroboran que el modelo resuelve la necesidad crítica de integrar la seguridad a nivel gerencial, pues, en conjunto, estos hallazgos reafirman que las recomendaciones planteadas están diseñadas para ofrecer una estructura formal y un lenguaje común que resonará y tendrá eco en las directivas y en la alta dirección. Esto, a su vez, facilita la asignación de recursos y promueve una cultura de responsabilidad compartida, lo cual es esencial para el éxito y la sostenibilidad de cualquier programa de ciberseguridad en una industria tan esencial como la flexográfica.

Pregunta 9. ¿En qué nivel considera Ud. que los controles y medidas sugeridos son apropiados para la protección de sus redes internas/externas (incluido el acceso a Internet)?

Los hallazgos reproducidos en la ilustración siguiente, revelan una aceptación prácticamente total (100% de las respuestas concentradas entre los niveles 4 y 5) por parte de las organizaciones de la industria flexográfica en cuanto a la apropiación de los controles y medidas sugeridas para la protección de sus redes internas/externas., pues, como se detalla en la imagen, con un 58% de las respuestas ubicadas en el nivel 4 y un 42% en el nivel 5, las empresas

encuestadas indican que las soluciones técnicas propuestas para el dominio de seguridad de redes son vistas como apropiadas y necesarias.

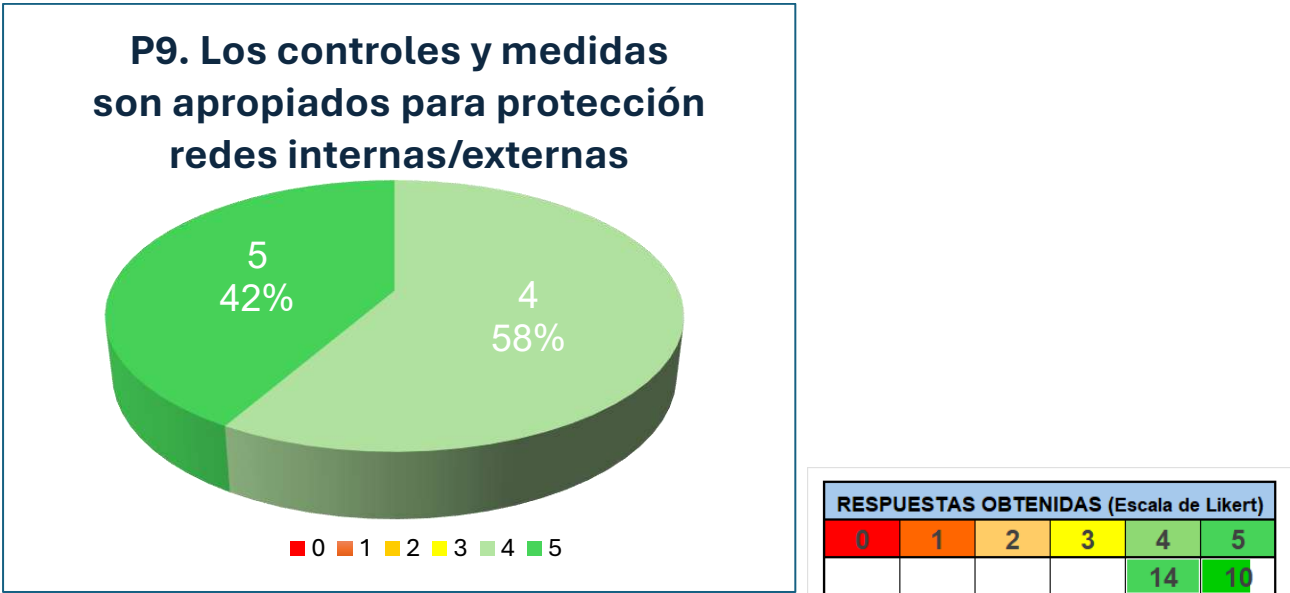


Fig. A8.9

Resultados obtenidos en la novena pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la novena pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

En efecto, esta distribución altamente favorable, indica que el sector reconoce la vital importancia de contar con defensas robustas en el perímetro, como firewalls avanzados y sistemas de detección de intrusiones, para controlar el acceso a internet y segregar las redes internas críticas de la infraestructura IT asociada a la gestión de la cadena de producción crítica de la industria. Este consenso absoluto en los niveles superiores valida de forma contundente la eficacia técnica y la relevancia del dominio relacionado con la seguridad de las redes planteado como elemento clave dentro del modelo de ciberseguridad desarrollado, pues, al confirmar que las empresas consideran que los controles propuestos son adecuados para gestionar los flujos de tráfico y mitigar las ciberamenazas que provienen tanto del exterior como del interior de la red, los resultados corroboran que el prototipo cibernético protectivo diseñado ofrece soluciones técnicas sólidas y alineadas con las necesidades operativas de la industria en estudio.

En conjunto, estos hallazgos reafirman que, las recomendaciones planteadas en esta área son percibidas como prácticas, escalables y esenciales para mantener la confidencialidad, integridad

y disponibilidad de la seguridad de la información de los activos claves de la infraestructura IT asociada a la cadena de producción crítica del sector flexográfico.

Pregunta 10. ¿En qué nivel considera Ud. que su adopción contribuiría a la reducción de impactos negativos ocasionados por ciberataques?

El análisis de los resultados (100% de las respuestas concentradas entre los niveles 4 y 5, presentados en la imagen anterior), evidencian la máxima convicción por parte de las organizaciones de la industria flexográfica acerca del impacto directo y positivo del modelo de ciberseguridad propuesto en la reducción de las consecuencias negativas de un ciberataque, pues, como se observa, con un 63% de las respuestas ubicadas en el nivel 5, esta pregunta registra el porcentaje más alto de respuestas en el nivel de máxima valoración, lo que indica que el objetivo fundamental del modelo, es decir, la mitigación de riesgo y sus impactos, es visto como una meta altamente alcanzable.

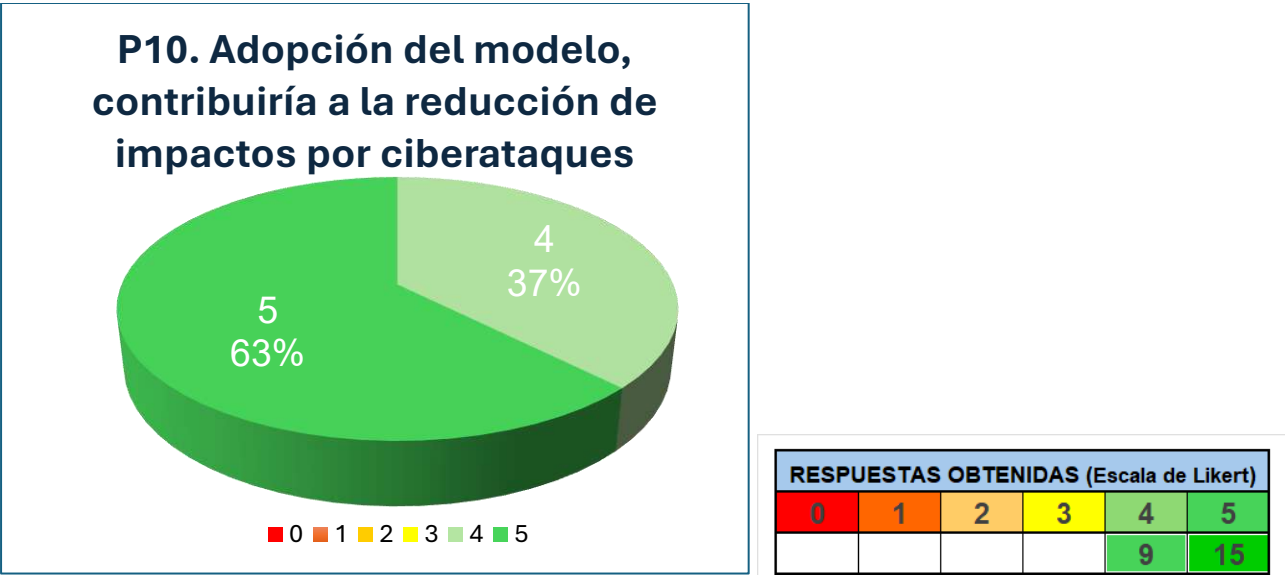


Fig. A8.10

Resultados obtenidos en la décima pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la décima pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

Este resultado refleja que los encuestados perciben la adopción integral de los controles sugeridos por el prototipo cibernético protectivo, no solo como medidas preventivas, sino como un escudo eficaz y efectivo para limitar pérdidas financieras, operativas y de reputación tras un

incidente, lo cual conlleva, a la larga, a la reducción del riesgo informático. Al efecto, este consenso absoluto y la marcada preferencia por el nivel 5 en las respuestas obtenidas, valida de manera contundente y definitiva el modelo de ciberseguridad propuesto, pues, al confirmar que las empresas y, en especial, las PYMEs, consideran que, su adopción propiciará una disminución significativa en los daños potenciales ocasionados por los ciberataques, los resultados establecen una fuerte correlación entre la implementación del prototipo cibernético de protección y la mejora de la resiliencia industrial.

En conjunto, los hallazgos reafirman que, las recomendaciones planteadas no solo son apropiadas a nivel de componentes individuales (como redes, backups o capacitación), sino que, además, su aplicación holística es percibida como la solución más eficaz y necesaria para proteger la continuidad operativa del sector flexográfico ante el creciente y sofisticado panorama de ciberamenazas que azota a las industrias esenciales, en la actualidad.

Pregunta 11. ¿En qué nivel considera Ud. que su adopción contribuiría al mejoramiento de la gestión de atención y respuesta de incidentes informáticos?

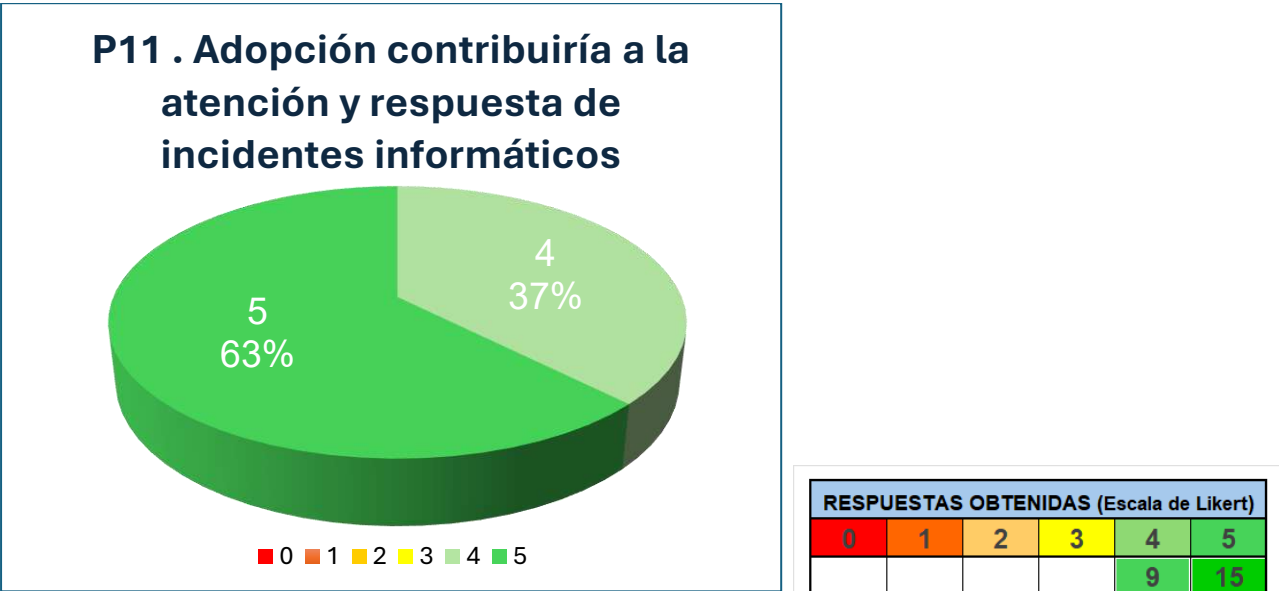


Fig. A8.11

Resultados obtenidos en la décimo primera pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la décimo primera pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico. Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

El análisis de los resultados obtenidos y presentados en la imagen anterior, con 100% de las respuestas concentradas entre los niveles 4 y 5, evidencian el alto nivel de convencimiento que genera la consideración del prototipo de ciberseguridad propuesto por parte de las organizaciones de la industria flexográfica acerca del impacto en la gestión de incidentes informáticos, pues con un 63% de las respuestas ubicadas en el nivel 5, esta los hallazgos derivados de esta pregunta igualan el porcentaje más alto de valoración máxima (Pregunta 10), lo que subraya la alta prioridad que tiene para el sector flexográfico, la capacidad de reaccionar de forma organizada, ordenada y técnica, ante las ciberamenazas. Al dicho efecto, este resultado refleja que las empresas y PYMES encuestadas perciben que la adopción del modelo de ciberseguridad desarrollado proveerá los procedimientos, roles y recursos necesarios para que la atención y respuesta a incidentes sea más eficiente, reduciendo el tiempo de inactividad y minimizando el daño tras un evento de seguridad.

Así pues, los resultados obtenidos validan de forma contundente la eficacia y efectividad operativa del dominio de gestión, manejo y respuesta a incidentes y, por extensión, del prototipo de ciberseguridad desarrollado, pues, al confirmar que, las empresas consideran que el marco de trabajo facilitará la ejecución de planes de respuesta probados, los resultados establecen que el modelo resuelve una necesidad fundamental para la continuidad del negocio y la resiliencia operativa, dado que, en conjunto, estos hallazgos reafirman que el prototipo cibernético de protección diseñado contribuye a la construcción de la capacidad de resiliencia tan necesaria para la industria flexográfica, mientras asegura que la organización pueda detectar, contener, erradicar y recuperar sus sistemas rápidamente, un factor decisivo para la protección de la infraestructura IT asociada a la cadena de producción crítica sectorial.

Pregunta 12. En general, ¿En qué nivel considera Ud. que el modelo de ciberseguridad propuesto protegerá la confidencialidad, integridad y disponibilidad de la seguridad de la información de su cadena de producción crítica?

Los resultados presentados en la gráfica anterior (100% de las respuestas concentradas entre los niveles 4 y 5) evidencian la más alta convicción, reportada por parte de las organizaciones encuestadas de la industria flexográfica, acerca de la capacidad del modelo de ciberseguridad propuesto, para proteger los tres (3) pilares fundamentales de la seguridad de la información

(confidencialidad, integridad y disponibilidad) de la infraestructura IT asociada a su cadena de producción crítica.

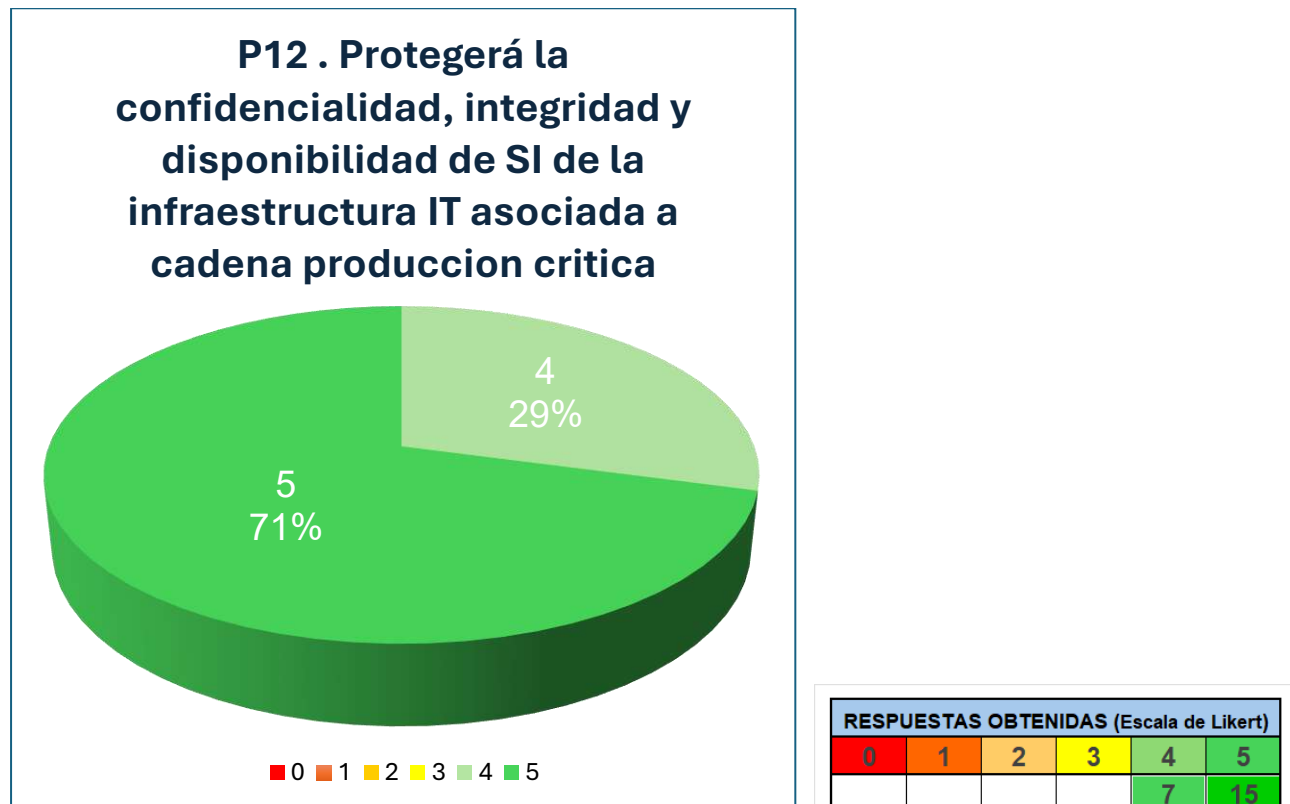


Fig. A8.12

Resultados obtenidos en la décimo segunda y última pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico.

Gráfico de tarta y tabulación detallada.

Nota: Resultados obtenidos en la segunda y última pregunta de la encuesta de validación final del modelo de ciberseguridad para el sector flexográfico.

Gráfico de tarta y tabulación detallada. Fuente: Autoría propia.

En efecto, los hallazgos derivados de la encuesta muestran que, con un 71% de las respuestas ubicadas en el nivel 5, esta pregunta registra el porcentaje más elevado de máxima valoración, lo que subraya que, el prototipo cibernético de protección diseñado es percibido como una solución eficaz y efectiva para blindar la información y los sistemas vitales de la cadena de producción. De hecho, este resultado refleja que las empresas encuestadas, y en particular, las PYMEs, tienen una alta confianza en que, la adopción integral del modelo de ciberseguridad desarrollado se traducirá directamente en la protección de los atributos esenciales de la información y, a la larga, se traducirá en disminución significativa del nivel de riesgo informático y el aseguramiento de la continuidad del negocio y la resiliencia operativa.

Este consenso absoluto y el porcentaje dominante en el nivel 5 en la escala de Likert, validan de manera concluyente y final el modelo de ciberseguridad desarrollado y presentado en esta tesis

de maestría, pues, al confirmar que las empresas consideran que la adopción del mismo es una vía segura, efectiva y eficaz para proteger los sistemas IT asociados a sus cadenas de producción críticas. En efecto, los resultados demuestran que el prototipo cibernético protector satisface la necesidad fundamental y final de la industria en términos de seguridad informática, pues, en conjunto, los hallazgos reafirman que las recomendaciones planteadas no solo son adecuadas a nivel de componentes aislados, sino que, su implementación integral es percibida como una estrategia adecuada para alcanzar una postura de seguridad que contribuya en la protección y aseguramiento de la confidencialidad, integridad y disponibilidad de los activos e infraestructura IT asociada a las cadenas de producción críticas del sector flexográfico.

Anexo Nro. 9

Autodiagnósticos finales obtenidos de los resultados de la encuesta de verificación del modelo de ciberseguridad (Autoevaluaciones según norma ISO 27001 y marco NIST 2.0 CSF)

Ver archivo Excel (Anexo Nro. 9 - .xlsx)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 3 - Actividad 3.2

Anexo Nro. 10

**Matriz de riesgo informático y mapa de calor
finales - Análisis y evaluación del riesgo
cibernético final basada en los resultados
obtenidos de la prueba de concepto
(encuesta de verificación) realizada para
validación del modelo de ciberseguridad**

Ver archivo Excel (Anexo Nro. 10 - .xlsx)

Instituto Tecnológico Metropolitano – I.T.M. – Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 3 - Actividad 3.2 - ENTREGABLE

Anexo Nro. 11

Nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI) New Industrial Cybersecurity Tinker Bell Cube (ICTBC) framework

Ver archivo PDF (Anexo Nro. 11 - .pdf)

Instituto Tecnológico Metropolitano - I.T.M. - Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 3 - Actividad 3.1

Nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI)

New Industrial Cybersecurity Tinker Bell Cube (ICTBC) framework

El nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI)

El “Cubo Campanito de la Ciberseguridad Industrial” (CCCI) es un nuevo marco técnico y pedagógico para facilitar la gestión de protección cibernética. Fue creado con el objetivo de apoyar las labores de ciberdefensa en PYMEs y empresas que operan cadenas de producción críticas en sectores industriales esenciales, como la industria flexográfica. La creación del CCCI se efectuó mediante la aplicación de un proceso de innovación ingenieril que, expandió, complementó, actualizó, adaptó, mejoró y fortaleció el tradicional y muy conocido cubo de McCumber de la seguridad informática de los años 90 y surgió, como un desarrollo complementario y colateral del trabajo de investigación, como recurso pedagógico, técnico y didáctico, para visibilizar y facilitar la comprensión, entendimiento y asimilación de la complejidad técnica del modelo de ciberseguridad a los gerentes, altas directivas y personal no especializado o sin mayor conocimiento en ciberseguridad..

Inicialmente, el marco CCCI se centró y se aplicó en el sector flexográfico, sin embargo, su diseño, estructura, flexibilidad metodológica, alcance y potencia didáctica, permiten adaptarlo con facilidad, como guía técnica de seguridad informática y como herramienta pedagógica, en otras industrias con similares características de criticidad en sus cadenas productivas. Esto se debe a que el CCCI facilita la comprensión, asimilación y adopción de los conceptos técnicos, actividades y funciones clave de la ciberseguridad en todos los niveles de una organización, promoviendo la protección y aseguramiento de la confidencialidad, integridad y disponibilidad de la seguridad de la información de las infraestructuras computacionales asociadas a la gestión de las cadenas de producción esenciales y difícilmente reemplazables. Complementariamente, el CCCI, por naturaleza y diseño, integra un enfoque pedagógico que ayuda a visualizar, asimilar y entender, con facilidad, los conceptos técnicos complejos de la seguridad informática, proporcionando los fundamentos y bases necesarias para una adecuada ciberdefensa en profundidad que, también, sea adaptable, efectiva y práctica para PYMEs y empresas del ámbito industrial.

En efecto, como se consideró anteriormente, la transformación digital ha generado profundos cambios en los procesos productivos e industriales. Al respecto, sectores como el flexográfico, encargado de producir envases, etiquetas y embalajes para industrias esenciales, esta evolución ha implicado la incorporación progresiva de tecnologías como la informática, la automatización, incluso los sistemas de control digital (SCD). Además, el internet de las cosas (IoT) y, más recientemente, la inteligencia artificial (IA) han arribado con fuerza y gran penetración a los sectores productivos industriales. Si bien estos avances han mejorado la productividad, también, han aumentado y agravado significativamente la exposición al riesgo cibernético de las industrias, especialmente, en las PYME, las cuales, a menudo carecen de estrategias de seguridad digital, formalmente implementadas.

En este sentido, el objetivo del Cubo Campanito de Ciberseguridad Industrial (CCCI) surgió como un resultado colateral e inesperado, pero, necesario y útil del trabajo de desarrollo de un modelo de ciberseguridad sectorial, estableciéndose como marco de estrategia pedagógica y técnica, para facilitar la comprensión, apropiación e implementación de los modelos de ciberseguridad industrial. Es importante resaltar que, aun cuando el CCCI nació de una investigación específica en la industria colombiana de impresión flexográfica, al igual que su antecesor, el cubo de McCumber, en realidad se trata de un marco de seguridad informática de ámbito universal y potencialmente aplicable a otros sectores industriales similares con cadenas productivas críticas. El marco CCCI propuesto se basa en el reconocimiento de un desafío industrial común: la complejidad técnica de los modelos de seguridad de la información y su limitada comprensión por parte de gerentes, directores y personal no especializado en ciberseguridad, lo que limita su potencial de adopción y aplicación organizacional.

Para superar este obstáculo, se diseñó el marco CCCI, una estrategia de visualización de modelos de ciberseguridad industrial, basada en fundamentos pedagógicos y didácticos, articulada a través de un proceso de innovación ingenieril, que dio como resultado la mejora conceptual del cubo McCumber de seguridad informática, propuesto hace más de tres décadas, en 1991, por el Ing. John R. McCumber, en un evento de la NCSC (*McCumber, 1991*) [59]. Se trata de un marco clásico de protección de la seguridad de la información ampliamente reconocido en el ámbito de las empresas y organizaciones. La propuesta consistió en actualizar y complementar el cubo original, ampliando sus dimensiones para representar y visualizar de forma clara y completa todos los componentes de un modelo de ciberseguridad industrial. Esta nueva versión se denominó Cubo Campanito de Ciberseguridad Industrial, CCCI, y fue concebida como una herramienta educativa y técnica para

facilitar la comprensión y adopción de un modelo específico de ciberseguridad corporativo entre gerentes, partes interesadas, directores senior y personal no especializado, en particular, empleados de operación y personal lego en la materia.

El desarrollo del CCCI surge de un enfoque investigativo que integró principios de ingeniería de procesos, seguridad de la información, pedagogía, didáctica e innovación conceptual, con el propósito de crear una solución comprensible, aplicable y replicable para la concientización, capacitación y toma de decisiones estratégicas en entornos de ciberseguridad industrial; traduciendo la complejidad técnica a un lenguaje accesible para personal no especializado y aportando valor técnico en contextos reales. Su diseño ingenieril garantiza alineación con estándares internacionales como NIST 2.0 CSF, la familia de normas ISO 27000 series y los CIS Controls, así como con buenas prácticas de ciberseguridad, lo que le permite enfrentar eficazmente los riesgos cibernéticos actuales. Consolidado como recurso técnico y pedagógico, el CCCI fortalece la resiliencia digital, la continuidad operativa y la sostenibilidad organizacional en sectores con infraestructura crítica, posicionándose como una propuesta de innovación educativa y de ingeniería aplicada que facilita la adopción de estrategias complejas entre personal no técnico, y establece las bases para su adaptación en otros sectores productivos clave para la economía real. Dicho lo anterior, es menester conocer el origen del cubo de McCumber que dio origen al nuevo marco CCCI, a saber:

El cubo de MacCumber de la seguridad informática original

El cubo de MacCumber de la seguridad de la informática, fue propuesta en 1991, durante la 14ava conferencia nacional de seguridad computacional (Washington DC; Estados Unidos), por el ingeniero americano John R, MacCumber, Capitán (retirado) de la Fuerza Aérea de los Estados Unidos (U.S.A.F.) que estuvo adscrito al Pentágono y fue analista de seguridad de la Agencia de Seguridad Nacional de los Estados Unidos (National Security Agency – N.S.A.), quién, en su ponencia “Information systems security: a comprehensive model” (*McCumber, 1991*) [59], basándose en su experiencia y amplio conocimiento y motivado en una ponencia del año anterior, en el mismo evento, donde se relevaba la importancia, necesidad y urgencia de desarrollar una estructura conceptual o modelo para el aseguramiento de la seguridad informática de fácil entendimiento, visible y práctica y, a este efecto, el autor se inspiró en el conocido y mundialmente famoso “Cubo Mágico” para generar un modelo integral de seguridad informática.

Al igual que el popular “Cubo Rubik” que, a su vez, fue desarrollado en 1974, por el arquitecto y escultor húngaro Erno Rubik, el Cubo de MacCumber de la seguridad informática se difundió rápidamente en el ámbito de la seguridad informática americana y mundial, popularizándose durante el periodo la década de los noventa (90s), pero, particularmente en eventos especializados entre 1991 y 1992. Mayores detalles se pueden consultar en las memorias de dicha conferencia nacional de seguridad computacional, disponibles en (McCumber, 1991) [59].

Antes de continuar, y con el ánimo de poner una cara conocida al modelo de MacCumber de seguridad informática, se puede resaltar que el recorrido del Ing. Capitán (retirado) John R. MacCumber, ha sido extenso en la seguridad informática. Hasta 2016, en lo último que se pudo indagar con técnicas OSINT, MacCumber se desempeñaba como Director de Defensa de la Ciberseguridad para Norteamérica de la organización internacional (ISC)² y entre sus funciones colaboraba con legisladores y congresistas, en el Capitolio de los Estados Unidos, aportando ideas estratégicas a comités nacionales e internacionales sobre cuestiones y aspectos críticos de ciberseguridad.

Como ya se mencionó, además de ser ingeniero de profesión, MacCumber es un oficial retirado de la Fuerza Aérea de los Estados Unidos y miembro, en categoría de Fellow en Criptología, de la Agencia de Seguridad Nacional de los Estados Unidos (N.S.A.). Durante su carrera militar, MacCumber sirvió en la Agencia de Sistemas de Información de Defensa (D.I.S.A.) y en el Estado Mayor Conjunto del Pentágono, en calidad de Oficial de Guerra de la Información durante la Guerra del Golfo Pérsico. Fue nombrado miembro Fellow de la (ISC)² en 2016. En 2019, MacCumber fue nombrado codirector de la National Initiative for Cybersecurity Education (NICE) de la compañía privada Training and Certifications (T&C) Subworking Group. No se tienen más noticias desde entonces y se presume que, actualmente, John R. MacCumber continúa activo en dicho cargo.



Fig. A11.1 John R. MacCumber.

Nota: Fotografía del Ing. Capitán (r) John R. MacCumber, experto en ciberseguridad y creador del cubo de MacCumber de la seguridad informática, imagen promocional tomada del web site oficial de la Conferencia RSA de 2016. Fuente: Tomado de [59].

MacCumber, con el objetivo de proporcionar un marco integral tangible, práctico y aplicable, para la seguridad informática, propuso un modelo de tridimensional de seguridad de la información basado en la idea de aprovechar tres (3) de las caras de dicho rompecabezas cubico. En este sentido, el origen del cubo de MacCumber de la seguridad de la informática responde a la necesidad de estructurar y visualizar los diferentes aspectos a proteger y de importancia crítica en seguridad informática.

En esencia, el prototipo de cubo de MacCumber de la seguridad de la informática, considera tres (3) dimensiones fundamentales en un sistema informático, todas necesarias de ser protegidas y aseguradas, entre ellas y de relevancia esencial para el asunto de estas tesis, se encuentra la dimensión de los objetivos de seguridad de la información, compuesta, fundamentalmente, por los tres (3) aspectos básicos de la triada de la seguridad de la información (tríada CIA por la siglas en ingles de confidentiality, integrity y availability), i.e., asegurar la confiabilidad, la integridad y la disponibilidad de un sistema informático. A esta dimensión, MacCumber agregó, la dimensión de la protección de los Datos en sus diferentes estados (almacenados, en tránsito y en procesamiento) y la dimensión de los mecanismos de defensa cibernética (tecnología, concientización, y políticas y procedimientos).

La propuesta efectuada por MacCumber se manifiesta el objetivo claro de facilitar la comprensión, el diseño, la implementación, el establecimiento y la evaluación de programas de seguridad de la información, consolidando una perspectiva adaptable y práctica, pero, sobre todo tangible, al interior de las organizaciones, lo cual tiene la utilidad de proporcionar una visión integral, comprensible y concreta, de los diferentes aspectos fundamentales que deben considerarse, para proteger efectiva y eficazmente la infraestructura computacional, las redes informáticas, los activos críticos y los datos en cualquier organización, pero, particularmente, aplicable al caso tratado referente a los sistemas informáticos asociados a la gestión de la cadena productiva crítica de una empresa del sector flexográfico.

En este punto, es importante hacer notar que, antes de su aparición, la seguridad informática se abordaba de manera fragmentada, enfocándose, principalmente, en la tríada CIA (confidencialidad, integridad y disponibilidad), sin integrar de forma explícita otros factores fundamentales como los estados de los datos y los mecanismos de protección. Y aunque el modelo de MacCumber se inspiró en principios de seguridad ya existentes, como el “Orange Book” del Departamento de Defensa de los Estados Unidos (1985) que establecía criterios para

evaluar la seguridad de sistemas informáticos, el Cubo de la Seguridad Informática de MacCumber amplió estos conceptos, como se observa en el papero con el trabajo conceptual del propio autor, al poner de relieve y en consideración, la premisa que no solo es importante lo qué se protege, sino, también, cómo se debe proteger y en qué estado de seguridad se deben encontrar los datos objeto de protección.

Todos, conceptos valiosos y esenciales para la seguridad de la información que, ante las circunstancias actuales, los autores de esta tesis de maestría, en su modelo de ciberseguridad basado en CCCI, extienden hasta incluir otros tres (3) aspectos fundamentales que son: cómo formalizar dicha protección (nivel dimensional de estándares internacionales), cómo aplicarlo a los entornos industriales (nivel dimensional de implementación operativa (A.I.E.)) y cómo proteger la infraestructura crítica de una industria (nivel dimensional de continuidad y resiliencia), como se verá, en mayor detalle, en los apartes siguientes.

Para mejor comprensión, seguidamente, se presentan y se explican en detalle, todas las dimensiones del cubo de MacCumber de la seguridad informática original, así como su respectiva extensión y modificación para formar y consolidar el nuevo marco CCCI, las cuales serán expuestas en profundidad, para ilustrar en completitud como se conforma el nuevo marco de ciberseguridad industrial CCCI. Nótese que, el cubo de McCumber original continua constituyendo la base del nuevo marco CCCI, pues, este último conserva vigentes las tres dimensiones originales del cubo de McCumber.

A este respecto, el cubo de MacCumber de la seguridad informática, está compuesto, en principio y originalmente, por tres (3) dimensiones imprescindibles de la seguridad de la información, cada una de ellas asociada, respectivamente, a cada una de las tres (3) caras laterales visibles de un “Cubo Rubik” y, en cada una de dichas dimensiones (o caras laterales del “cubo mágico de la seguridad informática”), se representan, a su vez, tres (3) aspectos claves, o categorías, en que se puede dividir cada una de las dimensiones generales, para su mejor desagregación, comprensión y aplicación práctica, como a saber, se puede observar en la Fig. A11.2 que se consigna a continuación:

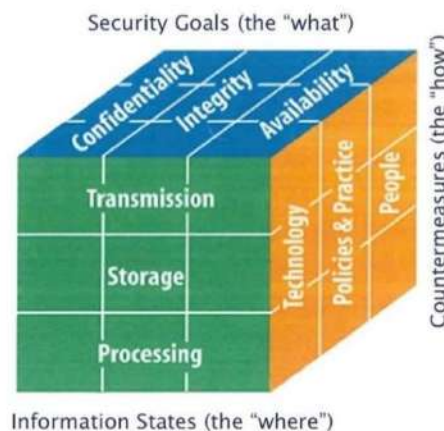


Fig. A11.2 Cubo de MacCumber de la seguridad informática. Presentación tridimensional cubica original.

Nota: Cubo de MacCumber de la seguridad informática. Presentación tridimensional cubica. (John MacCumber, NCSC-NSA, Estados Unidos, 1991). Fuente: Tomado de [60]

- **Principios fundamentales de la seguridad de la información (triada CIA de la seguridad informática):**

Como se observa en la Fig. A11.2, MacCumber integra la tríada CIA, asegurando la confidencialidad en cuanto a la protección contra accesos no autorizados; la integridad respecto a la precisión, no alteración y fiabilidad de los datos y, finalmente, la disponibilidad en cuanto al acceso permanente, oportuno y sin impedimento, a la información en el momento que un usuario, proceso o sistema, debidamente autorizado, la requiera para su respectivo uso o utilización.

- **Estados de la información (protección y la seguridad de los datos en sus diversos estados):**

Consecuentemente, también, MacCumber define las tres (3) formas en que los datos pueden existir dentro de un sistema, es decir, datos en reposo, cuando están almacenados; datos en tránsito, cuando se transmiten por la red; y datos en procesamiento, cuando están siendo utilizados por aplicaciones o programas, o siendo utilizados de algún modo. Para MacCumber, la gestión de la información es fundamental, concepto que en la actualidad continua vigente y representa una dimensión de seguridad valiosa e imprescindible.

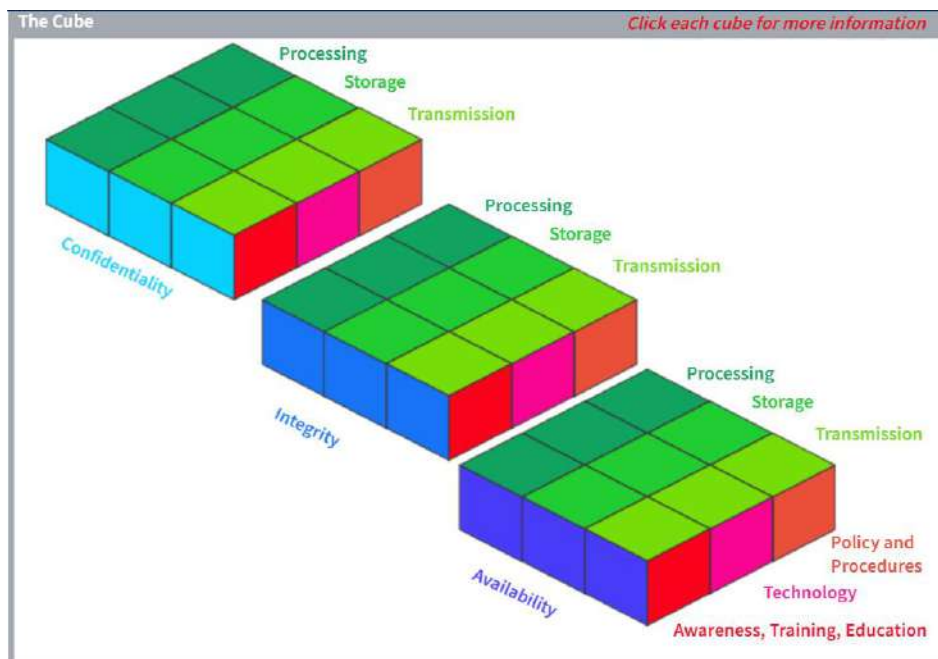


Fig. A11.3 Cubo de MacCumber. Desglose tridimensional de dimensiones y categorías originales.

Nota: Cubo de MacCumber de la seguridad informática – Desglose tridimensional de dimensiones y categorías. Fuente: Tomado de [61].

- **Medidas o Mecanismos de seguridad:**

Esta dimensión representa los controles y mecanismos de protección, que pueden ser de naturaleza humana, como la concienciación o la capacitación, tecnológica, relativa a hardware, software y medios técnicos como el cifrado, el uso de firewalls, IDS/IPS, etc; y, de políticas y procedimientos, como normativas, regulaciones, directrices, lineamientos, etc. McCumber consideraba, en aquel entonces, que estos aspectos eran fundamentales para la ciberseguridad y su visión se conserva de pleno en el nuevo marco CCCI.

De esta manera, el enfoque tridimensional, consolidado por MacCumber, en su cubo de la seguridad informática, permite visualizar cómo se deben implementar medidas de seguridad de la información en una organización teniendo presente los objetivos de la triada de la seguridad informática, la protección de los datos en sus diversos estados, y los mecanismos propios de la seguridad cibernética que garantizan una protección integral, sistemática y holística en las infraestructuras y en los sistemas de información.



Fig. A11.4 Cubo de MacCumber. Desglose bidimensional de niveles dimensionales y categorías originales.

Nota: Cubo de MacCumber de la seguridad informática. Desglose bidimensional de niveles dimensionales y categorías. Fuente: Autoría propia.

Así, se tiene que, el modelo del “Cubo de MacCumber de la Seguridad Informática”, detallado en la Fig. A11.4 (anterior) constituía una herramienta integral para aterrizar y otorgar tangibilidad al diseño de un modelo de ciberseguridad de aquella época, mientras que, por naturaleza, permitía asegurar su confiabilidad, su integridad y su disponibilidad. Además, protegía otros aspectos que son, igualmente, tan fundamentales, como necesarios, para la seguridad de la información de una organización. Sin embargo, su capacidad ha quedado limitada por el tiempo ante la complejidad, sofisticación y crecimiento de las ciberamenazas actuales.

A continuación, y con base en las ideas anteriormente consignadas, se presenta la extensión, actualización y mejoramiento del Cubo de MacCumber de la seguridad informática, en un nuevo marco denominado Cubo Campanito de la Ciberseguridad Industrial (CCCI), así como su

descripción detallada, la cual, conforma un nuevo marco de seguridad informática adaptado a las condiciones industriales y que permite lograr la consolidación, tangibilización y visualización del prototipo del modelo de ciberseguridad propuesto para el sector flexográfico, integrando, para ello, tres (3) nuevas dimensiones, a las tres (3) dimensiones originalmente propuestas por John MacCumber.

Al efecto, y con la finalidad de lograr una ciber-cobertura y una defensa a profundidad mucho más completa y robusta, acorde con las circunstancias actuales de digitalización industrial y, en particular, de los sectores productivos críticos de la economía real, se consideró necesario complementar, mejorar y actualizar, las tres (3) dimensiones propuestas originalmente por McCumber en su constructo conceptual de 1991, ampliando y extendiendo las capacidades de protección digital, en un nuevo y mejorado marco consolidado en un más completo y actualizado cubo de seguridad informática, específicamente orientado a las industrias esenciales: el CCCI o Cubo Campanito de la Ciberseguridad Industrial, que se muestra en la ilustración siguiente.

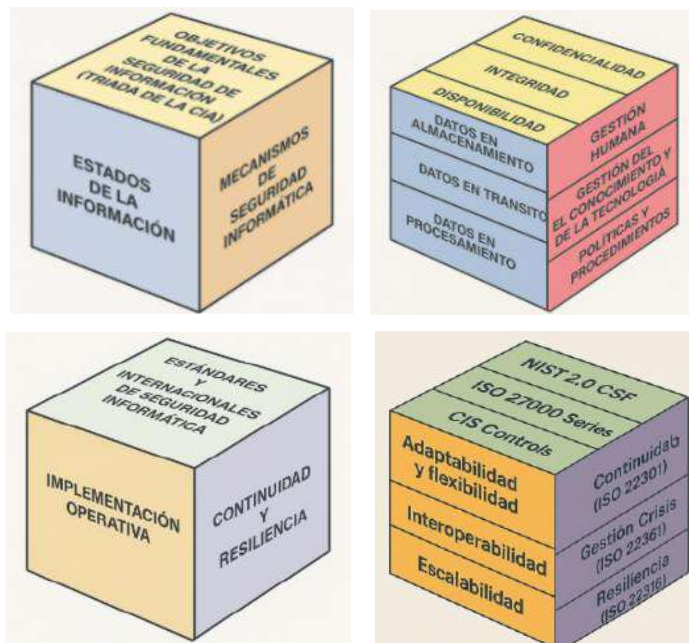


Fig. A11.5 Nuevo marco Cubo de Campanito de Ciberseguridad Industrial (CCCI).

Nota. Extensión, adaptación, actualización y mejoramiento del cubo de McCumber con enfoque en sectores industriales esenciales con infraestructuras de producción críticas. El CCCI está compuesto por todos los cubos de la imagen, incluida la contribución original de McCumber. Fuente: Autoría propia.

Las tres (3) nuevas dimensiones adicionales incorporadas al nuevo CCCI (estándares y referentes internacionales de seguridad informática; implementación operativa y continuidad y resiliencia), fueron el resultado de considerar las particularidades y condiciones muy especiales

de las industrias esenciales de la economía real con cadenas productivas críticas. En efecto, en este tipo de industrias, y sobremanera en sus PYMEs con limitados recursos para inversión en soluciones tecnológicas y escasez de personal especializado en ciberseguridad, la superficie de exposición al riesgo cibernético aumenta cada día, en razón a las tendencias en las ciberamenazas emergentes que reúnen alto grado de sofisticación, una mayor complejidad técnica, creciente aumento en la cantidad y la frecuencia de los ciberataques.

Las tres (3) nuevas dimensiones adicionales incorporadas en el nuevo marco CCCI y que, actualizan, adaptan, complementan y extiende el cubo de McCumber, ayudan a mitigar el riesgo digital, emergente y residual, en una infraestructura informática, incluyendo la protección ante ciberataques basados en ingeniería social, o generados con herramientas automatizadas implementadas con inteligencia artificial (IA), ayudando a defender y combatir, tanto intentos maliciosos incipientes, como también, amenazas emergentes.

El CCCI representa un escudo ante surgimiento y establecimiento de una billonaria industria de cibercrimen organizado, como, también, el *modus procedendi* de ciberdelincuentes, especializados en cibercrimen, ciberterrorismo y ciberguerra, cuyo accionar malicioso es significativamente peligroso, pues se trata de verdaderos profesionales, altamente entrenados y tecnológicamente avanzados en conocimiento técnico y que, adicionalmente, cuentan con grandes recursos, ya propios de sus organizaciones maliciosa, o cuya fuente es un fuerte e irrestricto patrocinio estatal.

De otra parte, el nuevo marco CCCI está conformado por las tres (3) dimensiones originales creadas por McCumber, a lo cual, se agregan tres (3) nuevas dimensiones ideadas y que están orientadas a fortalecer la protección cibernética industrial actual de las infraestructuras informáticas asociadas a la gestión de las cadenas productivas críticas (vale hacer notar que, el potencial de defensa en profundidad, que ofrece el CCCI, puede extenderse a muchos otros sectores fuera de la economía real). Así pues, el CCCI está parcialmente compuesto por las tres (3) dimensiones originales del constructo de (*McCumber, 1991*) [59], mostradas anteriormente, y que, a saber, son:

- Objetivos de Seguridad
- Estados de la Información, y
- Mecanismos de Seguridad Informática.

Actualmente, las dimensiones del constructo conceptual original de McCumber aún se mantienen vigentes como un reconocido pilar de la ciberseguridad. Sin embargo, también, es necesario reconocer que, ante la complejidad, sofisticación, automatización y crecimiento exponencial de las ciberamenazas y ante actores maliciosos supremamente organizados y con infraestructuras robustas y de última tecnología, que incluso utilizan herramientas de inteligencia artificial (IA), el constructo conceptual original de McCumber se encuentra superado y ya no es un marco suficiente para proteger y asegurar la seguridad de la información en sistemas informáticos asociados a las cadenas de producción críticas de industrias esenciales. Complementariamente, a las dimensiones anteriores se agregan, consolidando totalmente un nuevo cubo de seguridad informática (nuevo marco CCCI), las tres nacientes y nuevas dimensiones ideadas y presentadas, a continuación, en la Fig. A11.6, las cuales que están orientadas al propósito de robustecer la ciberseguridad industrial de la actualidad, y que, son:

- Estándares y referentes internacionales de amplia aceptación de ciberseguridad
- Continuidad y Resiliencia; y
- Implementación Operativa.



Figura A11.6. Dimensiones adicionadas en el nuevo marco CCCI.

Nota. Las 3 nuevas dimensiones de seguridad cibernética agregadas para expandir y actualizar el cubo de McCumber (Estándares y referentes Internacionales de ciberseguridad de amplia aceptación, Continuidad y Resiliencia, e Implementación Operativa) mejoran la ciberdefensa en profundidad y la protección de la seguridad de la información en entornos industriales críticos. La imagen presenta cada una de las nuevas subcategorías dimensionales de cada nueva dimensión propuestos por el CCCI. Fuente: Autoría propia.

En aras de ilustrar, con mayor detalle técnico, cada una de las dimensiones del nuevo marco CCCI, a continuación, se presentan los aspectos de protección y aseguramiento de la seguridad de la información, de cada nueva dimensión y la descripción, *grosso modo*, de cada una de las respectivas subcategorías de cada una de sus dimensiones protectivas:

- **Dimensión de los Objetivos de Seguridad** (*Confidencialidad, Integridad, y Disponibilidad*).

Esta cara del cubo, propuesta por McCumber, define qué se debe proteger. La *confidencialidad* asegura que la información solo sea accesible para usuarios autorizados; la *integridad* garantiza que los datos no sean alterados sin permiso; y la *disponibilidad* asegura que los sistemas y la información estén accesibles cuando se necesiten.

- **Dimensión de los Estados de la Información** (*Transmisión, Almacenamiento, y Procesamiento de Datos*)

Esta cara, también, ideada por McCumber, describe dónde se encuentra la información en cada momento. La información puede estar en estado de *transmisión* mientras los datos circulan, fluyen y se envían por redes. También, puede estar *almacenamiento*, cuando se guarda en dispositivos o sistemas, y, finalmente, los datos pueden estar en *procesamiento* mientras son manipulados o utilizados por programas y aplicaciones.

- **Dimensión de los Mecanismos de Seguridad Informática** (*Tecnología, Políticas y Procedimientos, y Factor Humano*)

Esta cara define cómo se protege la información con mecanismos específicos como salvaguardas y controles de ciberseguridad. McCumber planteó que las *tecnologías* incluyen herramientas y sistemas de seguridad necesarios para la operación y la ciberprotección; mientras que las *políticas y procedimientos* establecen las directrices, lineamientos, normas y controles organizativos. Finalmente, McCumber destacó que el *factor humano*, en su calidad de eslabón más débil en la cadena de seguridad informática, abarcan capacitación, conducta del personal y prácticas que reducen errores o riesgos internos.

Al aporte de McCumber, descrito antes muy *grosso modo*, se propuso incluir tres (3) nuevas dimensiones para completar y actualizar el cubo original. Dichas nuevas dimensiones fueron resultado de la aplicación de la metodología de investigación mostrada en la Fig. A11.6 (anterior) la cual condujo a una solución al problema investigativo de visibilización, facilitación del entendimiento y comprensión y asimilación de los conceptos de ciberseguridad por parte de los gerentes y personal no especializado en el área. Ver Fig. A11.7 (siguiente) con la estructuración completa.

INDUSTRIAL CYBERSECURITY TINKER BELL CUBE (ICTBC) <i>Cubo Campanito de la Ciberseguridad Industrial (CCCI)</i>			
MCCUMBER’S CUBE (ORIGINAL)		ADDITIONAL EXTENSIONS FOR THE CONSOLIDATION OF AN UPDATED FRAMEWORK	
DIMENSIONS (Originals)	CATEGORIES (Originals)	DIMENSIONS (Extended)	CATEGORIES (Extended)
FUNDAMENTAL OBJECTIVES OF INFORMATION SECURITY (CIA TRIAD)	Confidentiality	INTERNATIONAL STANDARDS AND REFERENCES FOR INFORMATION SECURITY	NIST 2.0 CSF
	Integrity		ISO 27000 Series
	Availability		CIS Controls
INFORMATION STATEMENTS	Data in Storage	OPERATIONAL IMPLEMENTATION	Adaptability and flexibility
	Data in Transit		Interoperability and integration
	Data in Processing		Scalability
COMPUTER SECURITY MECHANISMS	Human Factor	CONTINUITY AND RESILIENCE	Business Continuity (ISO 22301)
	Knowledge and technology management		Crisis Management (ISO 22361)
	Policies and procedures		Organizational Resilience (ISO 22316)
Two-dimensional view of the breakdown of the New ICTBC framework with dimensional levels and their respective categories.			

Figura A11.7. Estructura dimensional completa del nuevo marco CCCI.

Nota. Las seis (6) dimensiones completas del nuevo marco CCCI tres (3) de las cuales (lazo derecho) agregadas para expandir y actualizar y mejorar el cubo de McCumber. La imagen presenta cada una de las nuevas subcategorías dimensionales de cada una de las dimensiones propuestas en el nuevo marco CCCI. *Fuente: Autoría propia.*

Estas nuevas dimensiones adicionales se encontraron como producto de un proceso de innovación ingenieril aplicado durante el tránsito investigativo realizado. En este punto, también vale la pena aclarar y hacer notar que, este nuevo constructo conceptual (*el marco CCCI de Seguridad Informática*) surgió, como ya fue mencionado, como un resultado colateral durante la investigación realizada, pues, el objetivo general y principal de dicho trabajo era el diseño de un modelo de ciberseguridad para la protección y el aseguramiento

de la infraestructura informática asociada a la operación de la cadena productiva crítica de la industria flexográfica y que, realmente, el marco CCCI nació como herramienta de apoyo pedagógico y didáctico para visibilizar y facilitar la comprensión de los conceptos técnicos asociados al prototipo de protección cibernética desarrollado para dicho sector industrial.

En este contexto, las tres (3) nuevas dimensiones consolidadas y que dan forma plena al nuevo marco CCCI, son las siguientes:

- **Estándares y referentes internacionales ampliamente aceptados** (*Normas ISO 27000 series, marco NIST 2.0 CSF, y los CIS Controls*)

Esta nueva dimensión, reúne los marcos normativos que guían la madurez de la ciberseguridad, tan necesaria por estos días, en particular para la industria y sectores esenciales. La familia de normas ISO 27000 series (que incluyen normas como la ISO 27001, la ISO 27002, la ISO 27005 y la ISO 27035), el marco NIST 2.0 CSF (que incluye el factor de la gobernanza y funciones de seguridad como identificar, proteger, detectar, responder y recuperar) y, los CIS Controls (que incluyen los diez y ocho (18) CIS Controls categorizados en: el grupo de controles básicos, el grupo de controles fundacionales y el grupo de controles organizacionales), proporcionan principios, controles y prácticas que permiten estructurar una gestión de seguridad de la información sólida, adecuada, coherente, sirviendo como la base normativa del nuevo enfoque de ciberprotección propuesto por el marco CCCI.

- **Continuidad y Resiliencia** (*Normas ISO 22301, ISO 22361 e ISO 22316*)

Esta nueva dimensión define la capacidad de la organización para resistir, responder y recuperarse ante ciberataques o ante incidentes que afecten procesos industriales. Así mismo, la norma ISO 22301 establece los requisitos de continuidad del negocio, mientras que la norma ISO 22361 se encarga de gestionar eventuales crisis asignando responsabilidades y roles y asegurando los canales de comunicación. Y, de otra parte, la norma ISO 22316 propende por el fortalecimiento de la resiliencia, no solo operativa, sino, también, organizacional, asegurando que las operaciones críticas puedan mantenerse o restaurarse rápidamente tras una eventual interrupción. En otras palabras, esta dimensión propone, prepararse para lo peor, aguardando, siempre, lo mejor.

- **Implementación Operativa** (*Adaptabilidad y Flexibilidad, Interoperabilidad, e Integración, y Escalabilidad*)

Esta nueva dimensión completa todas las caras de nuevo marco CCCI, describe cómo se aterriza y se construye la ciberseguridad en la operación industrial diaria, pues incluye *la adaptabilidad y flexibilidad* para responder a cambios tecnológicos, técnicos o ante ciberamenazas si fuera el caso; la *interoperabilidad e integración* permiten coordinar sistemas IT con la infraestructura de la cadena de producción de forma cohesiva, alineada y sincronizada; mientras que, la *escalabilidad* permite que las soluciones crezcan en la misma y justa medida del crecimiento de las organizaciones y que estas se ajusten sin comprometer la eficiencia, ni tampoco la seguridad del entorno industrial.

Aplicación y modo de utilización del marco CCCI

Antes de continuar con la descripción de la forma en que puede ser utilizada la estructura conceptual del nuevo marco CCCI, cabe destacar que, su funcionamiento y operación son similares a los del cubo de McCumber de seguridad informática original, ya que el mejoramiento realizado con la ampliación de tres (3) nuevas dimensiones con sus respectivas categorías, además de extender y robustecer la idea de McCumber, complementa y actualiza el marco original de su creador.

Esto se logró sin alterar en absoluto su concepción funcional, tanto técnica como pedagógicamente, convirtiéndola en una útil herramienta de protección cibernética. Como se observó antes, la Fig. A11.3 muestra la intersección de las diversas subcategorías dimensionales para el cubo de McCumber de la seguridad informática y, que constituye, en esencia, el mismo *modus procedendi* para utilizar y aplicar el nuevo marco CCCI.

En otras palabras, cualquier usuario interesado puede seleccionar al menos dos de las dimensiones del nuevo marco CCCI y realizar una superposición (utilizando el concepto de los Diagramas de Venn) de dos (2) o más (y hasta seis (6)) diferentes subcategorías dimensionales, encontrando la mejor opción y los factores de protección fundamentales en el sistema informático real. Por ejemplo: confidencialidad con formación, integridad con las normas de la serie de normas ISO 27000, continuidad o resiliencia con cualquier estado de la información, etc.

Esta superposición permite interceptar, con el CCCI, hasta seis (6) diferentes aspectos de ciberseguridad de interés para una organización. También, según se desee o se requiera, se pueden interceptar dos (2) o más subcategorías dimensionales y así cada empresa puede ir avanzando en las especificaciones de su modelo de ciberseguridad.

En términos de ciberprotección y respecto a la seguridad informática de una organización o empresa, el funcionamiento es análogo al que se puede observar, para el constructo original de McCumber, en la animación digital tridimensional implementada en E-Mate 2.0 y disponible en el web site de (*NCYTE Center, 2024*) [61] y cuyos conceptos técnicos complementarios son presentados allí mismo.

Anexo Nro. 12

Estructura metodológica de investigación que condujo a la creación del nuevo marco Cubo Campanito de la Ciberseguridad Industrial (CCCI)

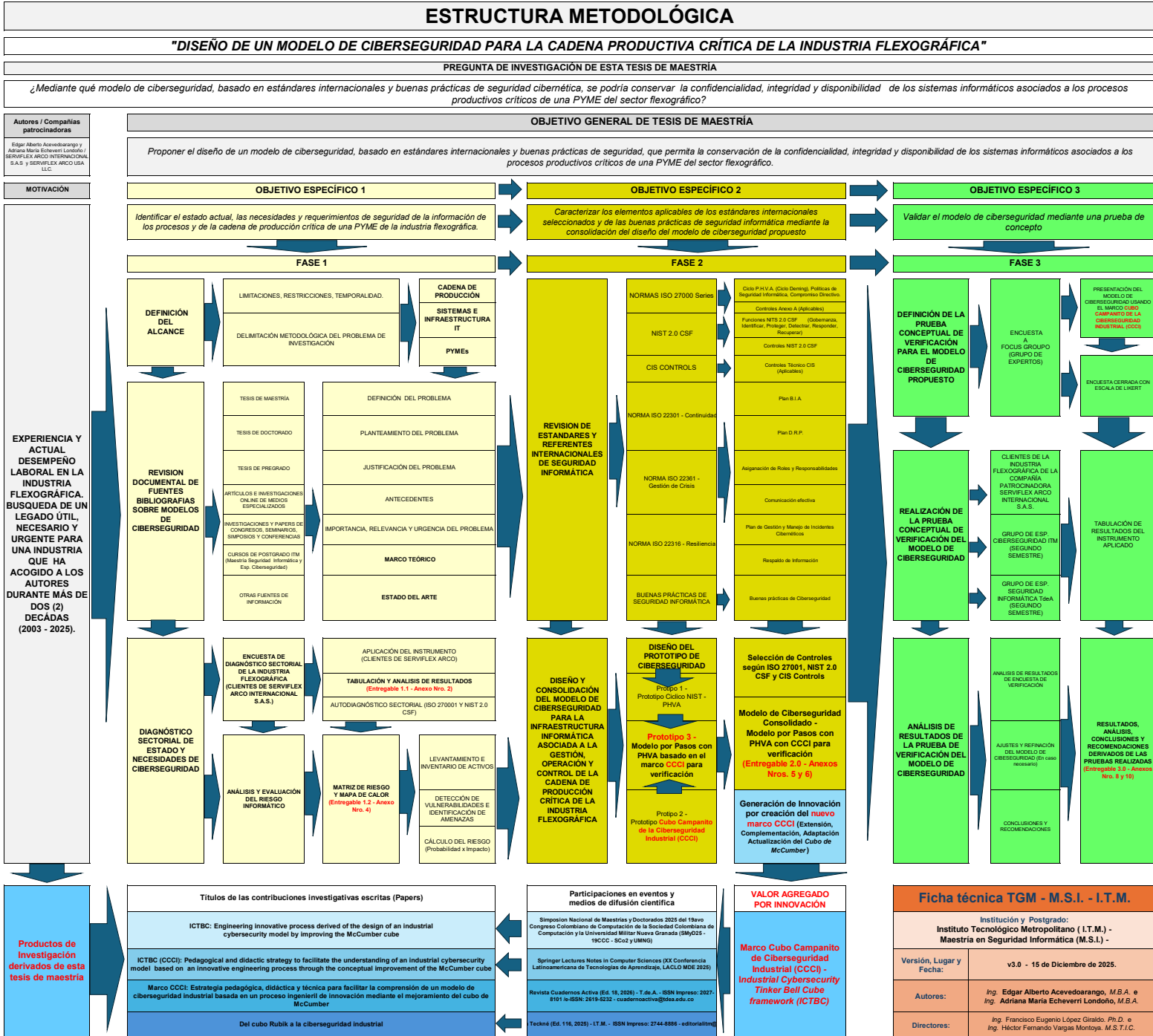
Ver archivo PDF (Anexo Nro. 10 - .pdf)

Instituto Tecnológico Metropolitano – I.T.M. – Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 2 - Actividad 2.2 y FASE 3 – Actividad 3.2



Anexo Nro. 13

**Productos de esta tesis de maestría en
seguridad informática.**

**Artículos publicados, o confirmados y a
publicar, en revistas indexadas.**

Ver archivo PDF a continuación con los siguientes artículos:

Instituto Tecnológico Metropolitano – I.T.M. – Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 4 y FASE 5

**Artículos publicados, o confirmados y a publicar,
en revistas indexadas.**

Productos de esta tesis de maestría en seguridad informática.

“Del cubo Rubik a la ciberseguridad industrial”.

La Tekné. ed. 116. No. 2025-2. Ed. Fondo Editorial ITM. ISSN: 2744-8886. Medellín, Colombia (2025).

“ICTBC (CCCI): Pedagogical, didactic and technical strategy to facilitate the understanding of an industrial cybersecurity model based on an innovative engineering process through the conceptual improvement of the McCumber cube”.

Springer Notes in Computing Sciences. Vol. (A confirmar). No. (A confirmar). Ed. Elsevier. ISSN: A confirmar. e-ISSN: A confirmar. Medellín, Colombia (2026)

“Marco CCCI: Estrategia pedagógica, didáctica y técnica para facilitar la comprensión de un modelo de ciberseguridad industrial basada en un proceso ingenieril de innovación mediante el mejoramiento del cubo de McCumber”.

Revista Cuadernos Activa Vol. 18 (A confirmar). No. 1(A confirmar). A confirmar (Ed.T.deA.). ISSN Impreso: 2027-8101. E-ISSN: 2619-5232. Medellín, Colombia (2026).

“ICTBC: Engineering innovative process derived of the design of an industrial cybersecurity model by improving the McCumber cube”.

Revista Universidad Militar Nueva Granada (A confirmar) Vol. (A confirmar). No. (A confirmar). Ed. U.M.N.G. ISSN: A confirmar. e-ISSN: A confirmar. *Memorias del SNMyD 2025 del 19CCC de la SCo2.* Bogotá, Colombia (2026).



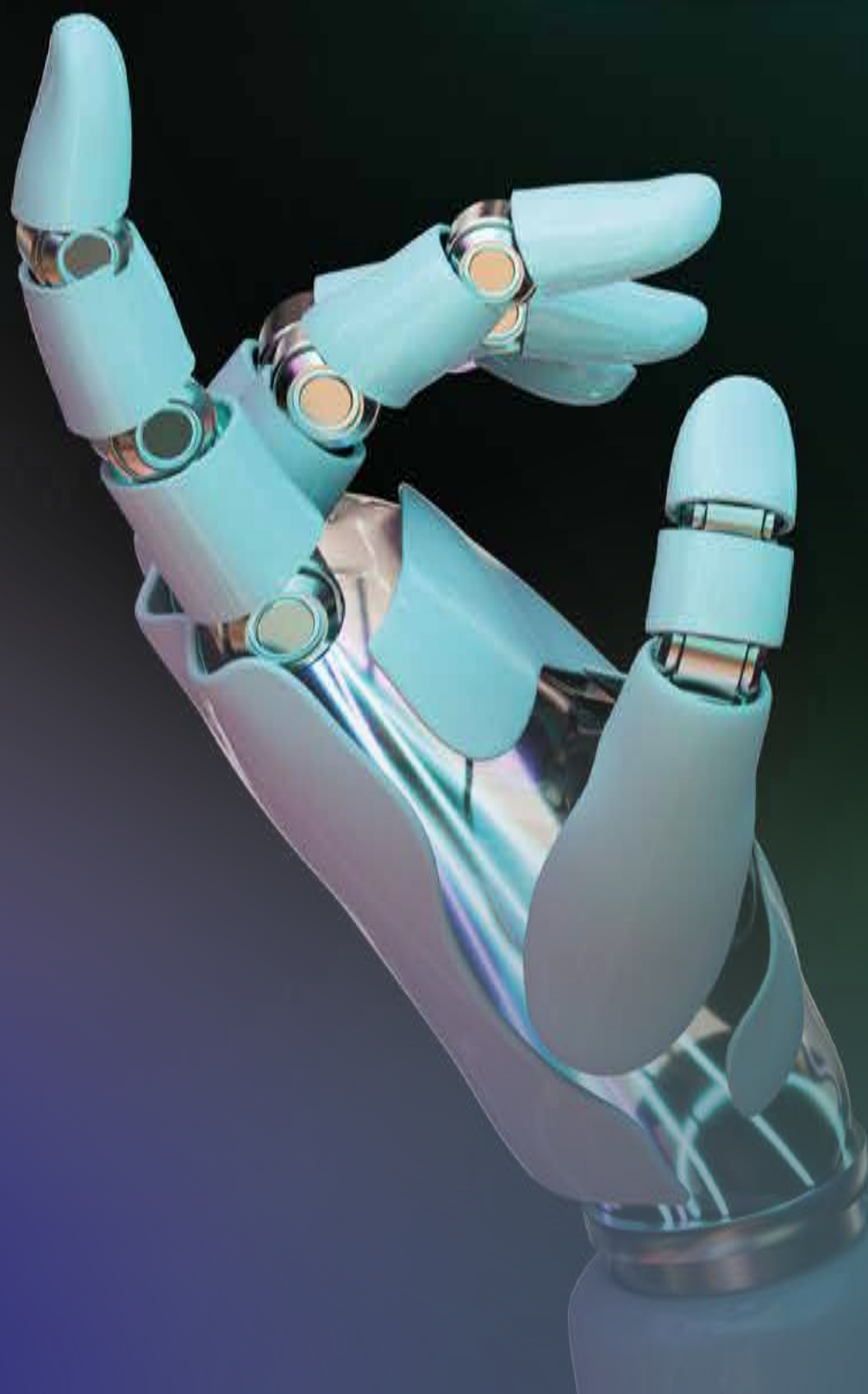
Institución
Universitaria
Reacreditada en Alta Calidad



Editorial
ITM

La Tekhné

/// ISSN 2744-8886 /// Edición 2025-1 /// No. 116



ITM
Somos la



PÁGINAS

06 - 09

Editorial. Mucho por hacer

[Editorial ITM](#)

10 - 16

Del cubo Rubik a la ciberseguridad industrial

[Edgar Alberto Acevedoarango - Adriana María Echeverri Londoño](#)

18 - 25

Bioseñales contra la depresión

[Juan Carlos Granada-García - Sebastián Roldán-Vasco](#)

26 - 35

Café con mucílago

[Juan Pablo Colorado - Jonathan Donado - Paula Andrea Osorio - Maria Elena Maldonado - Sarah Ruth Rothlisberger](#)

36 - 41

¿Algo nos mira?

[Claudia Betancur-Henao - Robison Buitrago-Sierra](#)

42 - 48

De las algas a la bioingeniería

[Magdelly Stephanya España Villota - Robison Buitrago-Sierra](#)

50 - 56

Electrodo de disco rotatorio

[Manuela Agudelo Calderón - Andrés Felipe Vargas Ramírez](#)

58 - 61

Una taza de ciencia

[Paula Andrea Buriticá Macías - Sarah Ruth Rothlisberger Booth](#)

62 - 67

De desecho a energía

[Jeferson Pinzón Chavarro](#)

La Tekhné

RECTOR

Alejandro Villa Gómez

VICERRECTOR DE DOCENCIA

Hernán de Jesús Salazar

VICERRECTOR DE INVESTIGACIÓN

Johnson Garzón Reyes

COMITÉ EDITORIAL

Mauricio Vanegas Gil

Director de Biblioteca, Extensión Cultural y Editorial ITM

Clara María Mejía Zea

Profesional Universitario Editorial ITM

Valeria Puerta Tamayo

Editor de mesa

CORRECCIÓN DE ESTILO

Martha Cecilia Caballero Jerez

Alejandro Vega Carvajal

DISEÑO Y DIAGRAMACIÓN

Manuela Escobar Ortiz

Mauricio Raigosa Álvarez

Marcela Londoño Agudelo

INFORMACIÓN CARÁTULA

Tomada de Freepik. Licencia libre.

INSTITUCIÓN UNIVERSITARIA ITM

Reacreditada en Alta Calidad,

adscrita al municipio de Medellín

www.itm.edu.co

Campus:

Robledo: Calle 73 N° 76A - 354

Fraternidad: Calle 54A N° 30 - 31

La Floresta: Calle 47A N° 85 - 20

Prado: Carrera 51 N° 58 - 69

Castilla: Carrera 65 N° 98A - 75

<https://www.itm.edu.co/la-tekhne/>

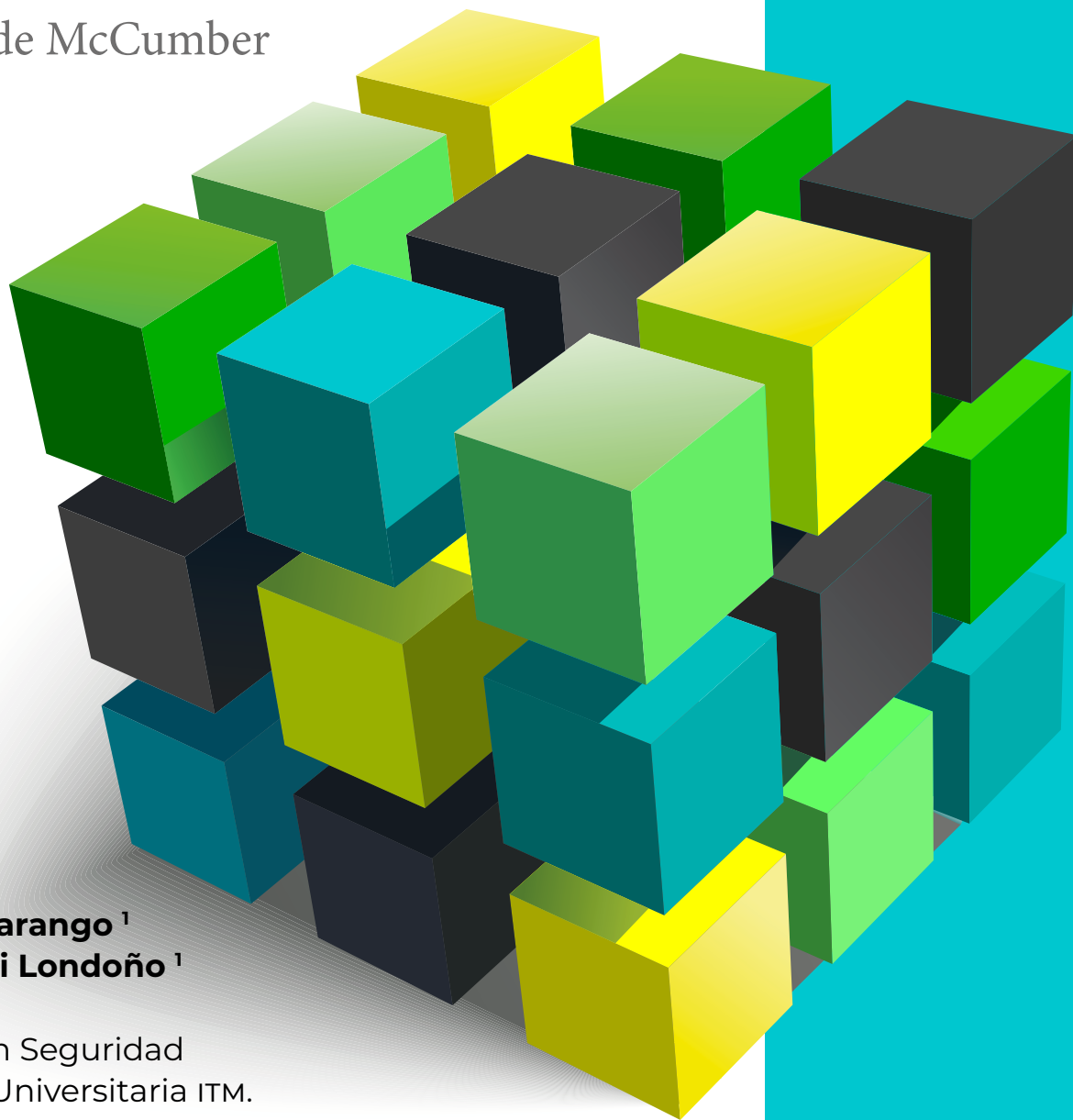
Contacto: editorialitm@itm.edu.co

La Tekhné es el periódico
institucional del ITM.

Las opiniones y noticias publicadas en él son
responsabilidad exclusiva del autor o autores, haciendo
uso de la libertad de expresión que las directivas de
la Institución Universitaria otorgan al trabajo de sus
estamentos académicos y administrativos.

Del cubo Rubik a la ciberseguridad industrial

Innovación ingenieril mediante la
extensión del cubo de McCumber



Edgar Alberto Acevedoarango¹
Adriana María Echeverri Londoño¹

¹Estudiantes, Maestría en Seguridad
Informática, Institución Universitaria ITM.

La industria flexográfica cumple un rol imprescindible en la producción de empaques, envases, cajas, etiquetas y otros insumos necesarios para las cadenas de suministro esenciales de otras industrias igualmente críticas como la alimentaria, la farmacéutica y la de bienes y productos de primera necesidad. Por su carácter difícilmente reemplazable, este sector enfrenta cada vez mayores amenazas cibernéticas que representan un reto para todas sus empresas.

Quisimos diseñar un modelo de ciberseguridad para la infraestructura informática asociada a la gestión de la cadena productiva crítica del sector flexográfico colombiano, con especial enfoque en las pequeñas y medianas empresas PYMES. Esta iniciativa busca fortalecer la protección de la seguridad de la información, garantizando su confiabilidad, integridad y disponibilidad en una industria esencial para el país.

El desarrollo del cubo Campanito de ciberseguridad industrial, CCCI (Industrial Cybersecurity Tinker Bell Cube o ICTBC, por sus siglas en inglés) [1], es una propuesta de innovación que adapta y amplía el marco conocido como cubo de McCumber de la seguridad informática [2].

La creciente automatización, digitalización e integración de sistemas de control digital (SCD) [3], junto con la adopción acelerada de tecnologías como el internet de las cosas (IoT) y la inteligencia artificial (IA) en los procesos y en las cadenas productivas, ha elevado los riesgos cibernéticos en el sector flexográfico, evidenciando la necesidad de adoptar modelos robustos de ciberseguridad industrial. Esto es urgente debido a la sofisticación, complejidad e incremento en la cantidad y frecuencia de los ciberataques que cada día comprometen más la continuidad operativa y la resiliencia industrial, lo que afecta la confidencialidad, integridad y disponibilidad de la seguridad de la información de las infraestructuras informáticas, en especial, de aquellos sistemas computacionales asociados a la gestión, operación y control de sus cadenas de producción críticas.



Figura 1. Plana típica de la industria flexográfica y su cadena de producción crítica, tomado de [4].

Materiales, métodos y metodologías de investigación

Nuestro trabajo se desarrolló como parte de una tesis de maestría en Seguridad Informática. Nuestra investigación se estructuró mediante una metodología por fases, organizada en tres etapas sucesivas y articuladas, que permitieron avanzar, de forma gradual y ordenada, para la obtención de los resultados.



Fase 1. Diagnóstico sectorial.

Se identificaron el estado actual y las necesidades de seguridad de la información en la industria flexográfica.



Fase 2. Análisis técnico e innovación.

Se revisaron estándares y referentes internacionales de seguridad informática y se consolidó un prototipo de ciberseguridad mediante un proceso de innovación ingenieril que complementó, extendió, adaptó y actualizó el marco conocido como cubo de McCumber de la seguridad informática.



Fase 3. Validación.

Se aplicó un instrumento metodológico a un grupo focal de expertos, con el fin de lograr la retroalimentación necesaria para verificar la eficacia y efectividad del prototipo cibernético y efectuar los ajustes necesarios para consolidar su versión final.



Fuente: Freepik. Licencia libre.

Un nuevo cubo mágico para la seguridad digital de la industria

Como parte del proceso, mejoramos y actualizamos el reconocido cubo de McCumber, un modelo marco de ciberseguridad que, en su momento, representó una propuesta innovadora. Este se inspiró en el popular cubo de Rubik o cubo mágico, muy de moda en los años noventa. El cubo de la seguridad informática, como también se le conoce, fue ideado, por el ingeniero J. R. McCumber, exintegrante de la Fuerza Aérea de los Estados Unidos (USAF), la Agencia de Seguridad Nacional (NSA) y la Iniciativa Nacional para la Educación en Ciberseguridad (NICE). Originalmente, McCumber propuso asociar las tres dimensiones fundamentales de la seguridad informática de la época con las caras laterales de un cubo mágico en su reconocido marco de seguridad cibernética.

De esta manera, tanto los objetivos de la seguridad de la información —conocidos como la tríada de la CIA: confiabilidad, integridad y disponibilidad— como los estados de la información (datos en tránsito, datos en procesamiento y datos en almacenamiento), y también, los mecanismos o contramedidas de seguridad informática —la tecnología, el factor humano y su capacitación, así como las políticas y procedimientos de ciberseguridad— quedaron vinculados con tres de las caras laterales de un cubo. Este antiguo marco de ciberseguridad consolidó las ideas básicas de protección y defensa cibernética de manera efectiva, eficaz y didáctica, acorde con las necesidades digitales de la época, de manera fácilmente comprensible, incluso para personas no especializadas en el área. No sobra mencionar que fue un éxito claro en su tiempo, constituyéndose como base de la ciberdefensa de la época.

Sin embargo, debido a los avances tecnológicos y a la evolución constante de las condiciones de seguridad cibernética, tras varias décadas, se hace necesario actualizar y fortalecer el marco original del cubo de McCumber. Con el fin de proteger de forma adecuada al sector industrial, en particular a las PYMES, se requiere una versión mejorada, ampliada y contextualizada a los desafíos actuales.

Este trabajo dio como resultado la creación del ccci. Es una propuesta novedosa que retoma la idea original de McCumber, pero la amplía, la adapta y la actualiza. Surgió de un proceso ingenieril de mejora en el que se incorporaron tres dimensiones de seguridad digital, diseñadas para enfrentar los desafíos cibernéticos específicos en los entornos industriales con infraestructuras productivas críticas.



Para lograrlo, el ccci aprovecha las tres caras restantes, que McCumber no había considerado, y añade tres dimensiones clave: los estándares y referentes internacionales ampliamente aceptados de seguridad informática (que incluyen el marco NIST 2.0 CSF, la familia de normas ISO 27000 series y los CIS controls); la aplicación operativa (adaptabilidad y flexibilidad, interoperabilidad e integrabilidad, y la escalabilidad) muy necesaria en la actualidad; y, finalmente, la continuidad y la resiliencia, fundamentales para los ámbitos industriales y, particularmente, en lo que respecta a procesos o cadenas productivas críticos y que se apoyan en normas como la ISO 22301 de continuidad del negocio, la ISO 22361 sobre gestión de crisis y la ISO 22316 de resiliencia organizacional.

El marco de ciberseguridad ccci representa una propuesta innovadora, pertinente y especialmente adecuada para la protección digital de la industria flexográfica; llega en un momento

crucial y, aunque conserva las ideas centrales de McCumber, robustece la defensa cibernética en profundidad, reduciendo de forma significativa los riesgos informáticos para las empresas, en particular para las PYMES, que suelen contar con recursos, personal y tecnología limitados.

Además, entre sus valores agregados se destacan dos aspectos. Primero, su diseño puede ser adoptado por otros sectores industriales similares al flexográfico con procesos o cadenas productivas críticos. Segundo, al igual que su predecesor, funciona como una excelente herramienta didáctica, pedagógica y de capacitación, que facilita la comprensión del modelo de ciberseguridad y su adopción por parte de gerentes, directivos y personal no especializado. Esto, sumado a su rigurosidad técnica, lo convierte en una herramienta cibernética para hacer seguimiento, evaluación, auditoría y mejoramiento de un sistema informático, de forma eficiente y efectiva.

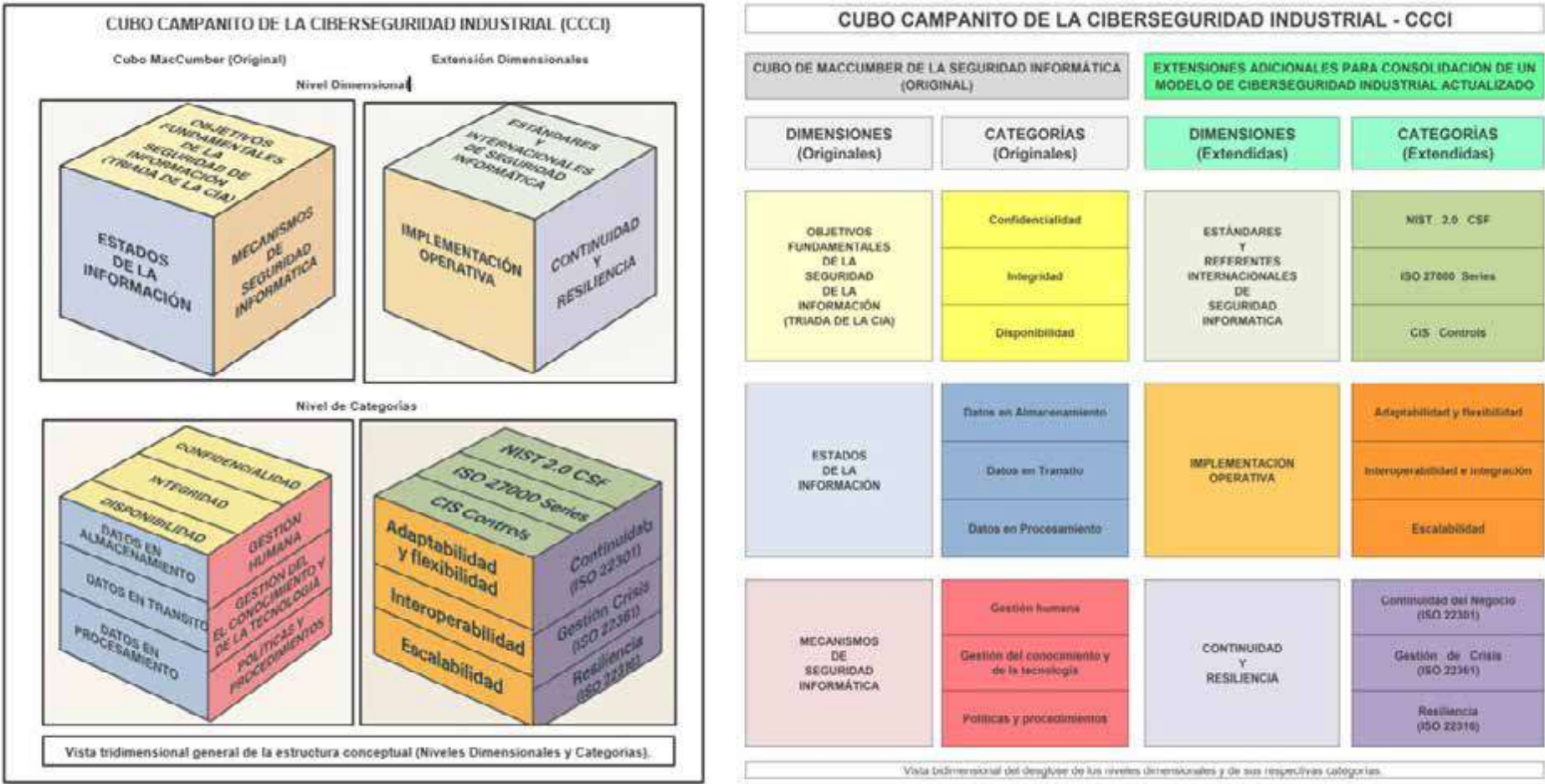


Figura 2. Cubo Campanito de la ciberseguridad industrial (ccci), versión completa, elaboración propia, adaptada de [1].

CONCLUSIONES

Nuestra investigación permitió demostrar que la industria flexográfica enfrenta un nivel creciente de riesgo cibernético, impulsado por la automatización, la digitalización acelerada y la adopción de tecnologías emergentes, como la integración de sistemas de control digital y la incorporación de IoT y AI en sus procesos productivos.

Este panorama, sumado al incremento en la sofisticación, complejidad y frecuencia de los ciberataques, confirma la urgencia de adoptar modelos robustos de ciberseguridad que no solo protejan la infraestructura tecnológica, sino que garanticen la continuidad operativa y la resiliencia de las cadenas de producción críticas de este sector esencial de la economía real.

Así, CCCI representa una innovación ingenieril y metodológica que incorpora nuevas y necesarias dimensiones de seguridad digital, orientadas a la protección cibernética integral de la industria, basada en estándares internacionales, aplicación operativa (adaptabilidad, interoperatividad, escalabilidad) y un aspecto esencial: la continuidad y la resiliencia digital, tan propias de las industrias con procesos críticos.

En términos prácticos, y como valor agregado, el marco CCCI no solo aporta a la innovación, sino que facilita la adopción y comprensión del modelo de ciberseguridad por parte de las directivas y del personal no especializado. Igualmente, es una herramienta replicable en otros entornos industriales, lo que refuerza su contribución al fortalecimiento de la competitividad y la sostenibilidad empresariales en sectores productivos estratégicos.

«El modelo puede ser entendido y aplicado por personas no expertas, incluyendo operarios, técnicos y personal administrativo».





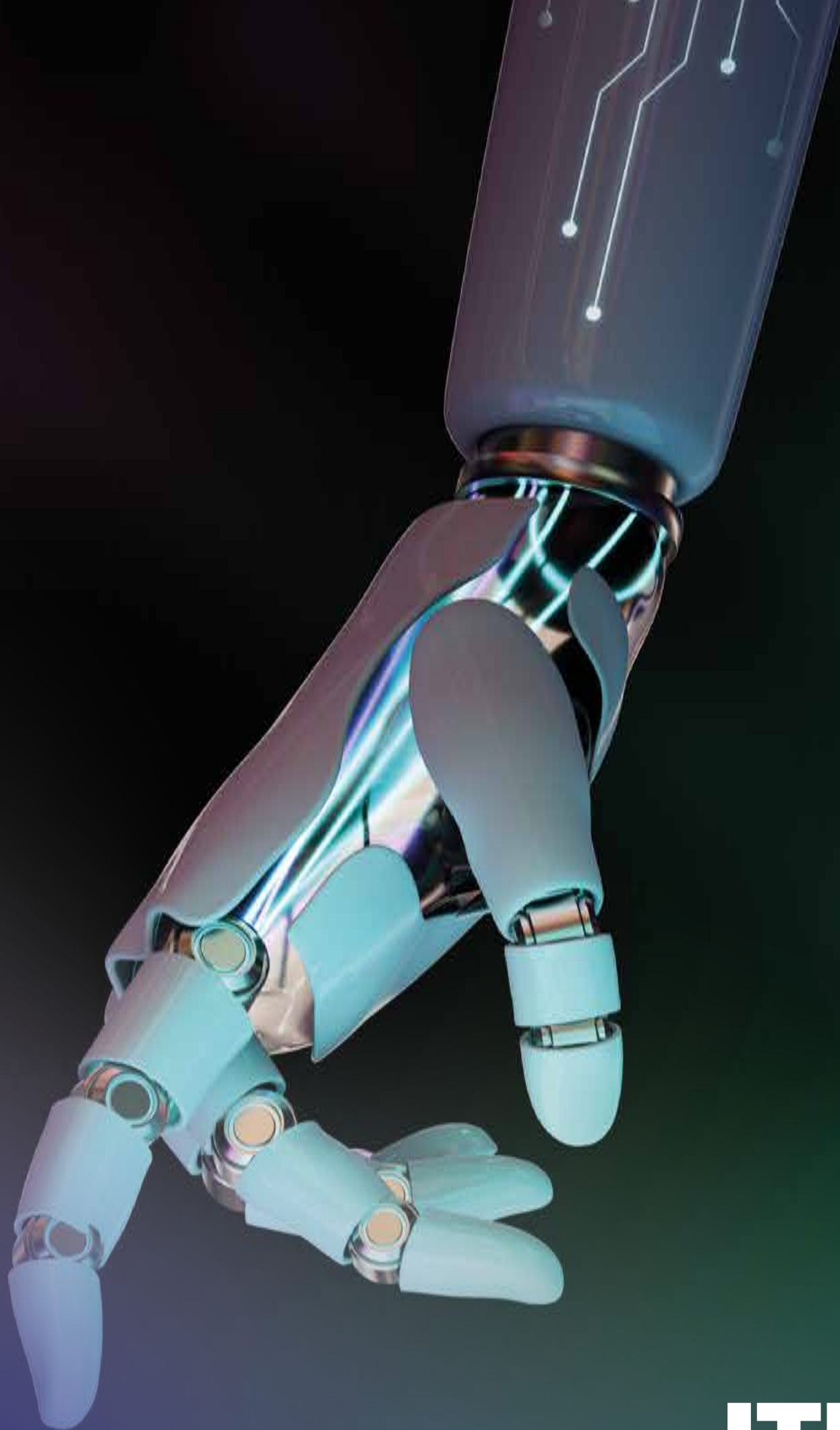
Agradecimientos

Los autores expresan su agradecimiento a Serviflex Arco Internacional S.A.S. (empresa patrocinadora), al ITM, a los ingenieros Héctor Fernando Vargas Montoya, Francisco Eugenio López Giraldo, Juan Fernando Hurtado Rivera, Leonel Marín, Sergio A. Álvarez G., Juliver Gil Herrera, Juan F. Puerta, Carlos Julio Escobar Noreña, Elizabeth Rodríguez Acevedo, Alicia Osorio Builes, Eduard Alberto García Galeano, Martha Cecilia Caballero Jerez, a la Editorial ITM; al rector del ITM, Alejandro Villa Gómez y a los diversos docentes, compañeros y profesionales, así como al Politécnico Colombiano Jaime Isaza Cadavid, Sapiencia, Mintic, Cisco, IBM, AWS, Open AI, Microsoft, Oracle, Google y a todas aquellas organizaciones y personas que han contribuido, de una u otra manera, a nuestra formación como *ethical hackers* y profesionales de la ciberseguridad, incluidos *youtubers* creadores de contenido educativo en seguridad informática, campos asociados y afines.

Referencias

- [1] E. A. Acevedo Arango y A. M. Echeverri L., «Diseño de un modelo de ciberseguridad para la cadena de producción crítica de la industria flexográfica», Tesis de maestría, Seguridad Informática, Institución Universitaria ITM, Medellín, Colombia, 2025.
- [2] J. R. MacCumber, «Information Systems Security: A Comprehensive Model», in 14th National Computer Security Conference, Washington, D.C., USA, 1991, pp. 328-337. <http://csrc.nist.gov/publications/history/nissc/1991-14th-NCSC-proceedings-vol-1.pdf>
- [3] E. A. Acevedo Arango, «Sistemas de control digital en subestaciones eléctricas de alta y extralta tensión», Tesis de Ingeniería, Universidad Nacional de Colombia, Medellín, Colombia, 1997.
- [4] EnvaPack (17 de mayo, 2019). Establecimiento Gráfico Impresores continúa creciendo en el mercado de embalaje flexible con impresoras flexo de tambor central y máquinas laminadoras BOBST. [Online] Disponible en: <http://bit.ly/4p1KGCI>

Fuente: Freepik. Licencia libre.



ITM 
Somos la

ICTBC (CCCI): Pedagogical, didactic and technical strategy to facilitate the understanding of an industrial cybersecurity model based on an innovative engineering process through the conceptual improvement of the McCumber cube

Edgar Alberto Acevedoarango¹ [0009-0001-1339-0517] and Adriana María Echeverri-Londoño² [0009-0002-4525-076X]

¹Politécnico Colombiano Jaime Isaza Cadavid (P.C.J.I.C.), Medellín, Ant, 050022, Colombia.

²Instituto Tecnológico Metropolitano (I.T.M.), Medellín, Ant, 050034, Colombia.
eaa.researcher@gmail.com, amecheverril@yahoo.com

Abstract. The Industrial Cybersecurity Tinker Bell Cube (ICTBC), also known Cubo Campanito de Ciberseguridad Industrial (CCCI), is a new cybersecurity framework and a methodological, technical and pedagogical innovation derived from the design of a cybersecurity model tailored to the small and medium-sized enterprises (SMEs) in Colombia's flexographic industry, with applicability to other essential sectors with critical production chain. ICTBC framework emerged as result of a master's thesis in computer security, focused on the digital protection of computing infrastructures that operate critical production process and chains. Built upon an innovative engineering process that updates and extends the McCumber cube, the new ICTBC framework serves as conceptual and technical cybersecurity guideline for the design, development, adoption and implementation of digital protection prototypes in essential industries. Its double dimension enables the translation of complex cybersecurity concepts into accessible language for executives and non-specialized personnel, fostering understanding, adaptation, and integration of protection models across all organizational levels. Additionally of their natural and intrinsic technical value, the ICTBC framework can be considered like an open educational resource (OER) and learning object (LO), with the potential to strengthen cybersecurity culture in both academic and industrial contexts. Its structure supports active learning, conceptual appropriation and technical guideline and knowledge transference in critical production environments contributing to the development of resilient organizations. Thus, the ICTBC framework is positioned as a new benchmark for industrial cybersecurity that will promote the adoption of cyber protection models and awareness, education and learning of a strong information security culture in essential industries.

Keywords: Industrial's cybersecurity, ICTBC (CCCI), McCumber's cube.

1 Introduction

This research is based on the development of a magister's thesis in computer security [1] and introduces an innovative engineering process that implements improving, complementing and updating the McCumber cube [2]. Indeed, the digital transformation has generated profound changes in production and industrial processes as inferred from the work of [3]. According to [4], in sectors such as flexographic, in charge of producing packaging, labels and packaging for essential industries, this evolution has involved the progressive incorporation of technologies such as computing, automation, even digital control systems (DCS) such as those studied by [5], in addition to the Internet of Things (IoT) and, more recently, artificial intelligence (AI). Although these advances have improved productivity, they have also significantly increased exposure to cyber risk as stated by [6], especially in SMEs, which often lack cybersecurity strategies, technological resources and specialized technical personnel. Thus, the protection of IT assets associated with the production chain becomes a priority challenge in industrial sectors with critical productive infrastructure.

In this regard, the objective of the ICTBC as pedagogical and technical strategy was to facilitate the understanding, appropriation, and implementation of an industrial cybersecurity model specifically designed for the Colombian flexographic printing industry, but also, potentially applicable to other various industrial sectors. The ICTBC framework proposed is based on the recognition of a common challenge: the technical complexity of information security models and their limited understanding by managers, directors, and operational and administrative staff not specialized in cybersecurity, which limits their potential for adoption and organizational application.

To beat this obstacle, the ICTBC framework, a visualization strategy for the industrial cybersecurity model was designed, based on pedagogical and didactic foundations, articulated through an engineering innovation process that resulted in the conceptual improvement of the McCumber cube of computer security, proposed more than three (3) decades ago by Eng. John R. McCumber, at the NCSC event in 1991 [2], a classic cybersecurity model widely recognized in the field of companies and organizations. The proposal consisted of updating and complementing the original cube, expanding its dimensions to clearly and comprehensively represent all the components of the industrial cybersecurity model. This new version, ICTBC, was conceived as an educational and technical tool to facilitate understanding of the cybersecurity model between managers, stakeholders, senior directors and non-specialized personnel, in particular, operation employees, but also, keeping the technical utility of McCumber's cube.

The approach integrated principles of engineering, information security, pedagogy, didactics, and conceptual innovation, with the goal of building a comprehensible, applicable, and replicable solution for awareness, training, and strategic decision-making in industrial cybersecurity environments. The strategy translated the technical complexity of the cybersecurity model into a language accessible to individuals without further cybersecurity training, and its conceptual redesign provided added technical value in real-world contexts as a tool for information security protection, training, and assessment in organizations, as is consigned by [1].

In this regard, the applied engineering process guaranteed technical consistency and alignment with widely accepted and recognized international standards, such as the NIST 2.0 CSF framework [7], the ISO/IEC 27000 series [8] and the CIS Controls [9], and even, and very importantly, cybersecurity best practices, thus ensuring its capacity to address current cyber risks. The ICTBC was consolidated as a useful teaching and pedagogical resource for improving digital resilience, operational continuity, and organizational sustainability in the industrial sectors, serving as both a technical cybersecurity model and a pedagogical and teaching vehicle to understand the cyberdefense concepts. In short, this development gave rise to a proposal for educational and engineering innovation applied to a real-life cyber context in the industrial environment. The consolidation of the ICTBC demonstrates that the combination of cybersecurity, pedagogy, and engineering design can facilitate the adoption of complex cyber-strategies among non-technical personnel in an industrial environment, laying the groundwork for their adaptation to other key sectors and industries for the real economy.

2 Flexographic industry and cybersecurity

As can be inferred from the research work of [4, 10, 11, 12], the flexographic industry is a key sector of the real economy that is dedicated to the production of flexible and rigid packaging, boxes, labels, containers and packaging, all products that are part of the supply chains of other equally critical industries, such as food, pharmaceutical, goods and necessities. The industrial sector has some important production chains like flexible packaging, labels and corrugated, to produce containers, packaging, boxes, shrink sleeves, among other basic products for other logistics and supply chains. The incorporation of new technologies that require protection within the flexographic industry's production chain can be observed in the image extracted from [13]. Specifically, Fig. 1 illustrates a typical productive plant of the flexographic sector, where these emerging technologies are present.



Fig 1. Flexographic industry and its typical critical production chain. Source: Taken from [13].

According to [10], this industry is characterized by the use of the Anilox (Roller engraved with microcells used to transfer the ink to the substrate) and by other processes described in more detail by [4, 10, 11, 12], making flexography, today, a flourishing and necessary industry for society and the real economy due to its neuralgic and essential nature, demonstrated by the past Covid-19 pandemic, which revealed its status as a critical productive infrastructure. As an essential and complex production chain to replace industry, the flexographic sector faces growing cyber threats due to digitalization, automation and incorporation of technologies such as AI, IoT and DCS in its production processes, highly automatized, in the actuality.

On the other hand, and due to the above, the development of a cybersecurity model, based on international standards and good computer security practices, that protects and ensures the reliability, integrity and availability of the computing infrastructure associated with the management, control and operation of the production chain of flexographic industry [1] (ICTBC framework is potentially extendable to other industrial sectors with critical productive infrastructures), is of great relevance and priority, a task for which the methodological research work began with the realization of a diagnosis of the current state and requirements of cybersecurity in this industry through an instrument specifically designed and implemented for this purpose (sectorial diagnostic survey according the orientations and methodologic guide of [14, 15]).

Thus, the research findings supported the need to design an applicable, affordable cybersecurity model adapted to the operational reality of SMEs and companies dedicated to flexographic printing and whose production is dedicated to supplying other critical production chains. This cybersecurity prototype had to consider the critical nature of production processes and the urgency of ensuring operational continuity and the industry's resilience to disruptive cyber events, but also to technological failures, technical contingencies, calamities, or disasters related to its infrastructure and IT systems for managing and controlling the critical production chain. However, what was unexpected was the need to make this cybersecurity model understandable to managers, directors, and personnel not trained in cybersecurity, which led to the creation of the ICTBC, not only as a technical cybersecurity tool, but also as a pedagogical, didactical and educational tool for companies and, in special, for SMEs in the industry.

3 Materials, methods and research methodology

The research methodology implemented was based on the application of the scientific method, suggested by [16, 17], which guided, in a structured and rigorous manner, the process of inquiry and bibliographic review. Various sources of information were consulted, primarily the repositories of local and some international public and private universities. Several research papers were produced, many at the master's level and some even at the doctoral level. Furthermore, the design of the cybersecurity model for the flexographic industry was consolidated through the development of a phased methodology. To this end, several phases were structured into successive and articulated research phases, with activities and sub-activities, which allowed for the sequen-

tial, gradual, and timely collection of results. The achievements were consolidated in three (3) main phases: phase 1 of sectoral diagnosis of the state and needs of information security, phase 2 of analysis of international standards and references of computer security, and consolidation of the cybersecurity prototype, and phase 3 of validation of the model through a methodological instrument applied to an expert focus group.

The first methodological phase involved a sectoral diagnosis carried out through two activities: (1) a survey following the guidelines of [14, 15] to identify the sector's cybersecurity needs, and (2) the development of a risk matrix and heat map based on [18–20], supported by two self-assessments aligned with NIST CSF 2.0 [7] and ISO/IEC 27001 [8]. These inputs enabled the identification of key sector challenges and the definition of corresponding security controls. The second phase reviewed international standards and best practices—ISO/IEC 27000 [8], NIST CSF 2.0 [7], CIS Controls [9], among others—to extract foundational elements for designing the cybersecurity model. This integration resulted in the ICTBC prototype, conceived as both a technical defense-in-depth model to ensure information reliability, integrity, and availability in the flexographic production IT infrastructure [1], and a pedagogical tool for sector-wide adoption. In this methodological phase, the new ICTBC framework was born, like solutions to difficulties mentioned above. The third phase validated the model through: (1) defining a proof-of-concept mechanism via a survey administered to a sector expert group; (2) applying this instrument in accordance with [14, 15]; and (3) analyzing results and refining the model. The successful proof of concept confirmed the model's applicability, clarity, and feasibility, fulfilling the thesis's specific and general objectives regarding information security in the critical flexographic production chain.

In this context, is important to note that cognitive difficulty was identified, derived from two key factors. The first was related to the notion of a model, understood as an abstract conceptual structure. The second factor corresponded to an epistemological obstacle generated by the technical complexity inherent to a cybersecurity model, which is challenging for individuals without specialized knowledge. For these reasons, it was necessary to search for a pedagogical and didactic mechanism, that conserve technical and engineering value and would make the cybersecurity model and their complex technical concepts more accessible to managers, directors, operators, and other non-specialized personnel. As a result, the McCumber cube was identified as an ideal resource to facilitate its understanding and to apply to it an engineering innovation process based on its improvement (extension, adaptation, complementation and updating).

Consequently, and as a result, the ICTBC cybersecurity framework was conceived and created like indirect result of [1]. Overall, this methodology enabled the development of an adaptable and contextualized cybersecurity model that was technically robust, efficient, and effective, and, importantly, pedagogically understandable. Through a pedagogical strategy of engineering innovation, the model generated added value not only based on its cybernetic foundation under international standards, but also on its easy assimilation by organizational management and its practical adaptation to the organizational reality of the target sector through a process of conceptual

innovation. The pedagogical approach was key to ensuring its appropriation by both management and non-specialized personnel, while the engineering component guaranteed its technical soundness. It expects that the validation of the ICTBC confirmed its usefulness as a replicable tool in other industrial sectors with similar cybernetic needs.

4 ICTBC Framework: Industrial cybersecurity tinker bell cube

The research process identified an epistemological gap between traditional design of cybernetic security models and their applicability in real industrial environments, which motivated the conceptualization of a pedagogical and didactic tool that will integrate engineering principles, technical cybersecurity concepts and strategic visualization that is extensible to all types of industries with critical productive infrastructures. It derived in the ICTBC's creation like improvement and updating process of McCumber cube. The original McCumber's cube can be appreciated, with your three (3) basic dimensions in the following image, extracted of [2] (see Fig.2).

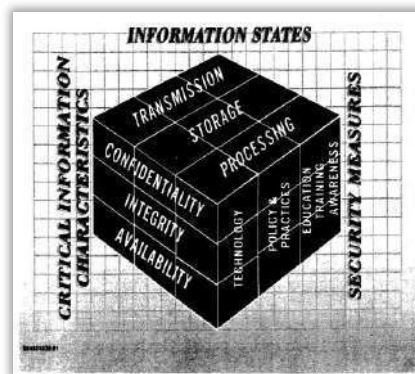


Fig. 2. McCumber's cube Source: Taken from [2].

Before detailing the ICTBC framework and its conceptual structure, it is worth highlighting that its functioning and operation is similar to the functioning and operation of the original McCumber cube of computer security, since the extension of three (3) new dimensions with their respective categories, in addition to improving, complements the tool, without altering in any way the functional conception, both technical and educational, of its original creator. In other words, any interested party can select at least two (2) of its dimensions and perform an overlay (use of the Venn's diagram) of two (2) different categories, finding the best option and the fundamental protection factors in the real computer system. For example: reliability with training, Integrity with ISO 27000 series standards, continuity and resilience with any state of the information, etc. This overlay allows intercepting, with the new ICTBC framework, up to six (6) different aspects of interest in terms of cyber protection, like

shows the following image extracted from [1], improving the cyber defense efforts of an organization. (see Fig. 3).

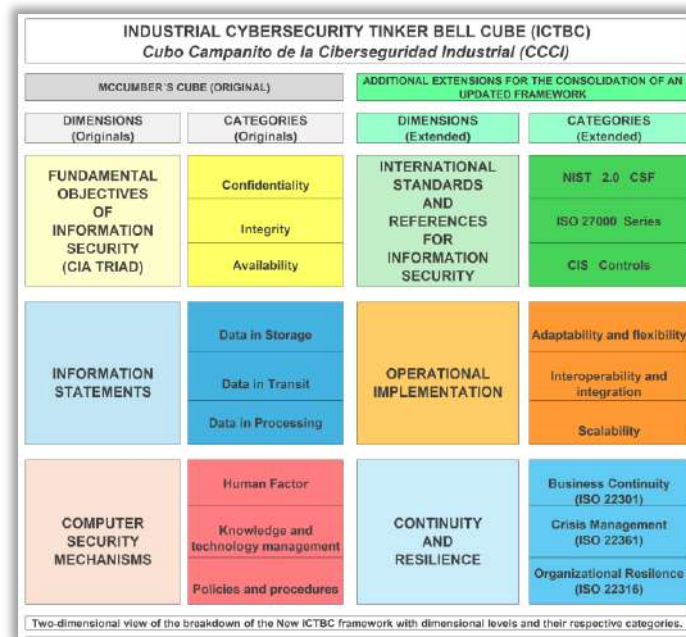


Fig. 3. New ICTBC (CCCI) framework structure. Source: Taken from [1]. Author's work.

These three (3) new additional dimensions were the result of considering the particularities of the industry, the trends in sophistication, complexity and increase in the frequency of cyberattacks and their automation, including malicious mechanisms and tools implemented with AI or factors such as the emergence of a billion-dollar industry of organized cybercrime and the malicious actions of groups of cybercriminals, specialized in cyberterrorism and cyberwarfare, highly trained and technologically advanced, who have their own resources or strong sponsorship from states and countries with ideologies opposed to the capitalist model, et al. At this point, it is also very important to highlight that, after considering the requirements of previous designs and facing the need to propose a structural and conceptual framework that would allow visibility, easy understanding and comprehension and the tangibilization of the cybersecurity model, the authors devised the ICTBC, which is presented above in the images that detail its construction and arrangement of dimensional levels and their respective categories.

To this end, and to achieve a more complete in-depth cyber coverage and defense, in accordance with the current circumstances of industrial digitalization and, in particular, of the critical productive sectors of the real economy, it was considered necessary to complement, improve and update, the three (3) dimensions originally proposed

by McCumber in 1991, expanding and extending the protection capabilities of its new and enhanced computer security's cube, as established above (see Fig. 3), and whose operation can be observed in detail in the E-Mate 2.0 three-dimensional animation of [21], making the exception that, said animation of [21], is exclusively designed to overlap the three (3) dimensions of the original McCumber cube (3 faces or sides only) and that, a mental and imaginative effort must be made, to visualize the overlapping of more than three (3) and until six (6) dimensions of the new ICTBC framework (4 to 6 faces or sides), like is proposed by [1] (See Fig. 3).

5 Industrial cybersecurity model's designs based on ICTBC framework: case of flexographic industry

On the other hand, and in order to consolidate the digital protection model for the flexographic industry —based on the review of international standards, good computer security practices, results of the sector diagnosis, risk matrices and heat maps, industrial design parameters and other elements of cyber defense in depth— and taking as a foundation the new ICTBC framework, the resulting cybersecurity prototype is presented in the following image extracted from [1] (see Fig. 4).

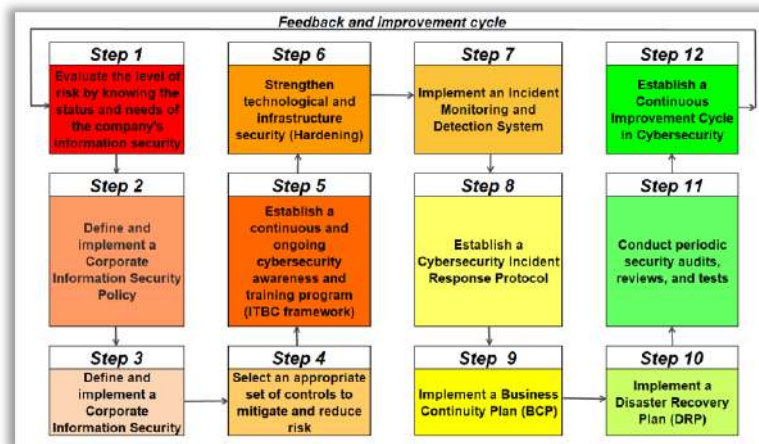


Fig. 4. Cybersecurity's model for flexographic industry based in the application of the conceptual guidelines of the new ICTBC framework. Source: Taken from [1]. Author's work.

6 Results

The extension, complementation, improvement, and updating of the original McCumber cube, consolidated through the creation of the ICTBC, strengthen all these characteristics and currently provide even greater advantages for cyberdefense in depth, which is added to the fact that it also favors its understanding and easy assimilation.

lation by personnel not specialized in cybersecurity, since, through simple didactic elements, it is possible to improve the knowability and significant learning of the cybersecurity model in organizations, by linking technical concepts with real information management situations derived from the new ICTBC framework.

Thus, from a purely pedagogical and didactically speaking perspective, the ICTBC cybersecurity model encourages progressive and structured understanding, transforming it into organizational knowledge, where each dimensional axis can be addressed individually, allowing its teaching to be modulated and adapted to different training levels (basic, intermediate, or advanced). For example, at introductory levels, one can start only with the explanation of the six (6) basic dimensions, i.e., the principles and objectives of information security, the states of information, and the strategies and mechanisms for computer protection and security, and gradually move forward with the incorporation of the various convergences of their respective categories, both two-dimensionally at the beginning and then three-dimensionally, until reaching a holistic understanding of all the capabilities that the ICTBC cybersecurity framework can offer. Its value as a teaching tool also lies in its ability to translate complex technical concepts into a visual and intuitive language, making it accessible to non-specialized audiences, such as managers, executives, process leaders, administrative staff, and even operators.

This, without neglecting its efficiency, effectiveness, and extensive cyber-protection capacity, makes the new ICTBC framework an ideal pedagogical and teaching resource for digital literacy in cybersecurity, ongoing training in companies and enterprises and, additionally, in training in similar industrial sectors with a high technological dependence and a delicate and fragile productive process, such as the flexographic industry. The model can serve as a basis for representing the components of a cyber-defense system aligned with international standards, highlighting its quality as an excellent pedagogical strategy for developing educational, academic, and research content, as is the case with the master's thesis in computer security, the subject of this research's job. Furthermore, from a cyber defense-in-depth perspective, both the McCumber cube and the new ICTBC can be combined with other international standards such as ISO/IEC 27001 [8], the NIST 2.0 CSF [7], or the CIS Controls [9], which reinforces their practical applicability and educational relevance. This complementarity strengthens their use in academic contexts for technical and postgraduate training, allowing apprentices, beginners, novices, and laypeople to easily understand and assimilate not only the conceptual principles but also their implementation in real-life environments, such as the flexographic industry.

The new ICTBC framework, as a teaching resource and pedagogical strategic tool, is consolidated and legitimized academically and educationally by linking it to recognized theoretical frameworks that support its applicability in technical and professional educational settings. For example, from a constructivist perspective, the new ICTBC framework promotes the active construction of knowledge by allowing students to model real-life industrial cybersecurity scenarios, integrating technical, organizational, and human variables in a contextualized analysis environment. This interaction stimulates critical thinking and problem-solving, pillars of meaningful learning.

Additionally, and in line with the meaningful learning approach proposed by Ausubel, the ICTBC facilitates the connection between new concepts and prior knowledge by presenting situations that require interpretation, decision-making, and strategic reflection. Its modular structure allows for the design of learning experiences aligned with instructional design principles, adaptable to different training levels, pedagogical objectives, and user profiles. This makes it a versatile tool for planning teaching sequences aimed at developing cybersecurity competencies. From a connectivist perspective, the ICTBC is projected as a knowledge hub that articulates technical, pedagogical, and organizational knowledge, promoting collaborative learning and continuous development in digital environments. This theoretical convergence legitimizes the ICTBC as a robust, scalable learning object aligned with the principles of open educational resources (OER) and learning objects (LO), with sufficient potential to be integrated into innovative training proposals such as those presented at LACLO Medellín 2025 and the National Magister and Doctoral Symposium 2025.

On the other hand, by translating complex technical concepts into accessible and didactic visual structures, the ICTBC framework is inherently and naturally presented as an innovative pedagogical tool for teaching industrial cybersecurity in organizations and other settings. Its three-dimensional design allows for the clear representation of protection layers, critical components, and risk vectors in industrial infrastructures, transcending the mere flexographic printing from which it originated and facilitating comprehension and easy understanding by non-specialists in the field of computer security. This ability to overcome abstraction and clearly visualize cybersecurity directly connects the ICTBC to learning theories such as constructivism, meaningful learning, and instructional design, which promote the active construction of knowledge, connections to prior experiences, and the contextualized application of technical knowledge.

To wrap up, from a methodological perspective, the ICTBC enables the implementation of active strategies that strengthen the teaching-learning process. It can be used in case studies to analyze real cyber incidents, as well as in collaborative projects where students design applied solutions, or in gamified dynamics that encourage exploration and decision-making. Furthermore, its modularity facilitates thematic segmentation, allowing for flexible learning paths adapted to different training levels as needed. In hybrid or virtual contexts, its interoperability makes it compatible with various educational platforms, as it can be adapted to the computing needs of e-learning platforms, expanding its reach and relevance in higher education programs, corporate training, and technical simulations.

Ultimately, the ICTBC, inheriting the virtues of the original McCumber cube represents a powerful pedagogical synthesis for teaching cybersecurity in a clear, step-by-step, and applicable manner. Its usefulness as a teaching aid makes it especially valuable for fostering the adoption of technical knowledge among non-specialized stakeholders and for consolidating informed decision-making processes regarding organizational cybersecurity and information security.

7 Discussion

Some very interesting aspects to discuss about the pedagogical contributions and the technical inputs about the new ICTBC framework are the following:

The new ICTBC framework expands upon the McCumber cube by offering a more accessible, modular, and pedagogically robust approach to cybersecurity. It simplifies complex technical concepts through visual and intuitive structures, making it easier for non-specialists, such as managers, operators, and administrative staff non-specialized, to understand and apply cybersecurity principles. Its design supports progressive learning, allowing educators to tailor instruction across basic, intermediate, and advanced levels. By linking technical dimensions to real-world information management scenarios, ICTBC fosters meaningful learning and strengthens organizational knowledge.

Grounded in educational theories like constructivism, meaningful learning, and connectivism, ICTBC promotes active knowledge construction, critical thinking, and contextual analysis. Its modularity enables flexible teaching strategies, including case studies, collaborative projects, and gamified learning. The framework aligns with international standards (ISO/IEC 27001, NIST CSF 2.0 and CIS Controls) and is adaptable to hybrid and digital platforms, making it suitable for industrial sectors with high technological dependence, such as flexographic printing, as well as academic and corporate training environments. Ultimately, ICTBC serves as both a cybersecurity model and a strategic teaching tool for building resilience and informed decision-making across organizations of essential industrial sectors.

8 Clarifications and future research work

Although this paper emphasizes the technical and pedagogical potential of the new ICTBC framework as a tool to visualize, understand, assimilate, and apply significantly complex technical cybersecurity concepts in industrial environments, it also acknowledges the limitations it still presents in its current level of adoption and real-world implementations. This is because the innovation derived from new ICTBC framework originated from a master's thesis, which, although completed, still lacks real-world applications, detailed descriptions of specific methodologies, and practical experiences in productive, learning, research, and professional environments, all of which are necessary for its effective appropriation by interested audiences.

To validate the new ICTBC's effectiveness, future research work must include empirical strategies such as case studies, pilot programs, and perception surveys involving both experts and non-expert personnel in SMEs and enterprises where the new ICTBC framework can be implemented. These efforts will help measure its impact on learning, adaptation, and decision-making in industrial environments and their technical effectiveness. Addressing the ICTBC framework's procedural and methodological gaps will strengthen its technical and pedagogical legitimacy, enabling the consolidation of metrics and evidence for broader application in the real industry. Ultimately, this will position ICTBC not only as a didactic resource but also as a robust cyber-

security framework capable of protecting critical production infrastructures and supply a real cyber-defense in depth for SMEs and enterprises.

9 Conclusions

The flexographic industry, recently recognized as critical due to the disruptions caused by the COVID-19 pandemic, faces increasing cyber threats that demand robust and scalable cybersecurity solutions. Its SMEs in particular, require models that strengthen defense-in-depth strategies and improve cyber protection capabilities. The growing sophistication and frequency of attacks have made this sector a target for malicious actors, highlighting the urgency of implementing effective cybersecurity frameworks tailored to its technological and operational vulnerabilities.

During the research process that led to the development of the new ICTBC framework, unforeseen challenges emerged, especially the need to make cybersecurity models understandable and applicable for non-specialized personnel. This need was not purely technical but pedagogical, prompting the quest of a didactic tool capable of bridging the gap between complex cybersecurity concepts and their organizational adoption. The new ICTBC framework, as an evolved, complemented, enhanced, updated and expanded version of the McCumber cube, responds to this challenge by offering a visual and modular structure that facilitates comprehension among managers, directors, and operational staff. While the original McCumber cube remains a valuable technical and educational framework, its limitations in addressing modern industrial cybersecurity needs, particularly in sectors with critical production infrastructure, necessitated its conceptual expansion. The new ICTBC framework introduces three (3) new dimensions and reconfigures the original McCumber's cube into a technical and pedagogical resource that supports both points of view, i.e., technical modeling and educational deployment. This dual function allows it to serve as a reference framework aligned with international standards (NIST 2.0 CSF, ISO/IEC 27000 series and CIS Controls) and as a training tool for digital literacy and organizational operational continuity and resilience.

The research also revealed that the main barrier to adopting cybersecurity models was not their technical design but the difficulty in understanding and assimilating them, especially among decision-makers and personnel without prior cybersecurity training. The human factor remains a central vulnerability in cyber defense, and the new ICTBC framework addresses this by promoting awareness, comprehension, and strategic thinking. Its pedagogical orientation enables the development of educational content that supports meaningful learning, critical analysis, and the integration of cybersecurity into organizational culture without forgetting the requirement of effective cyber-defense of the organization. Designed with modularity and interoperability in mind, the new ICTBC framework can be adapted to various learning environments, audience profiles, and technical depths. Its structure allows for flexible learning paths and thematic segmentation, making it suitable for academic programs, corporate training, and industrial simulations. By visually representing risks, threats, and defense layers, the ICTBC contributes to the formation of cyber-resilient personnel across

sectors, not only in flexography but in any industry where digital security is an essential point to attend.

The new ICTBC framework is based on key educational design principles that enhance its effectiveness as a specialized training resource. Its three-dimensional structure allows for high reusability, as it can be adapted to different levels of depth and technical or non-technical audiences. The model's modularity facilitates its decomposition into independent thematic components, allowing for the construction of flexible and personalized learning paths. Furthermore, its interoperability ensures compatibility with various digital platforms and teaching environments, facilitating its integration into academic programs, corporate training, or industrial simulations. In this sense, the ICTBC is geared toward achieving specific pedagogical objectives, such as understanding risks, the diverse cyber threats and vulnerabilities, and the various layers of cyber defense in depth as critical protection processes in industrial infrastructures. This contributes to the development of more aware, better trained, and strategically cyber-resilient personnel, not only in flexography but across all sectors and industries.

To wrap up, the new ICTBC framework is strategically integrated into the LACLO Medellín 2025 ecosystem, aligning with the principles of learning objects (LO) and open educational resources (OER). Its visual and accessible format transforms complex cybersecurity concepts into inclusive, scalable, and culturally relevant educational content. This positions the new ICTBC framework, as a replicable innovation in other industrial sectors, offering global applicability and reinforcing the role of pedagogical and didactics aspects in solving real-world cybersecurity challenges.

Acknowledgments. To: Serviflex Arco Internacional S.A.S.; I.T.M.; Politécnico Colombiano Jaime Isaza Cadavid; T.de.A.; Eng. Francisco Eugenio. López G., *Ph.D.*; Eng. Héctor Fernando Vargas M., *M.T.I.C.*; and Colombian flexographic industry.

10 Recommendations

The following recommendations provide a solid justification for incorporating the new ICTBC framework as a highly effective tool in cybersecurity. Its adoption is not only technically sound, given its operational alignment with the foundational logic of the original McCumber cube, but also strategically suited to industrial environments. The ICTBC stands out for its capacity to comprehensively address the specific cyber-risks faced by critical sectors operating under conditions of advanced automation, digitalization, and heightened exposure to cyberthreats. Unlike conventional models that focus narrowly on technological infrastructure, the new ICTBC framework integrates technical, operational, and organizational dimensions, along with the human factor. This multidimensional approach enables a robust defense-in-depth strategy tailored to the realities of industrial SMEs. It supports the design of customized controls, strengthens resilience across production chains, and promotes a cybersecurity culture that is both scalable and adaptable to diverse industrial contexts.

From a methodological standpoint, the ICTBC enables precise and contextualized identification of cyber risks, allowing for the mapping of specific vulnerabilities

across production processes, digital control systems (DCS), and environments involving IoT and artificial intelligence. One of its key advantages lies in its modular architecture, which supports the design and deployment of tailored cybersecurity controls aligned with the operational and technological capacities of each organization. This approach enhances the effectiveness of protective measures while avoiding unnecessary technical burden. As such, the ICTBC serves as a robust foundation for developing highly customized cybersecurity models suited to the needs of specific industrial sectors with critical production chains, i.e., the flexographic industry.

In addition, the ICTBC framework actively supports the reinforcement of organizational cybersecurity culture by incorporating pedagogical components that simplify the comprehension and internalization of its structure among non-specialized personnel. This approach enhances internal engagement and facilitates broader adoption across operational levels, contributing to the long-term sustainability of cybersecurity strategies. Moreover, the ICTBC effectively bridges international standards with localized industrial practices, delivering a solution that is scalable, interoperable, and adaptable to the evolving technical, regulatory, and operational demands of modern industrial cybersecurity environments.

References

1. Acevedoarango, E.A., Echeverri-Londoño, A.M.: From Rubik's Cube to Industrial Cyber-Security. *La Teckné*, I.T.M Institutional Magazine, 10–16, (2025). Last accessed: 25-11-2025. <https://repositorio.itm.edu.co/entities/publication/987b28b0-0c27-4d7f-a16d-6092805ec04b>
2. McCumber, J.R.: Information Systems Security: A Comprehensive Model. In: 14th National Computer Security Conference, pp. 328–337. NIST/NCSC, Washington D.C., USA (1991). Last accessed: 25-11-2025. <https://csrc.nist.gov/files/pubs/conference/1991/10/01/proceedings-14th-national-computer-security-confer/final/docs/1991-14th-ncsc-proceedings-vol-1.pdf>
3. Brito Acuña, G., Díaz Blanco, V.: Improving aeronautical cybersecurity processes through a maturity framework. *Rev. Cubana Cienc. Inform.* 17(Suppl.), 230–250 (2023). Last accessed: 25-11-2025. [https://rcci.uci.cu/?journal=rcci&page=article&op=view&path\[\]=2855&path\[\]=1156](https://rcci.uci.cu/?journal=rcci&page=article&op=view&path[]=2855&path[]=1156). DOI: 10.15446/dyna.v90n227.107420
4. Mejía Cortez, E.M.: The flexography market in Latin America. *Economic Situation Review*, Institute of Economic Research, San Salvador (2024). Last accessed: 25-11-2025. <https://revistas.ues.edu.sv/index.php/coyunec/article/download/423/355>
5. Acevedoarango, E.A.: Digital Control Systems in High and Extra-High Voltage Electrical Substations. Undergraduate thesis, National University of Colombia, Medellín (1997). URL no available.
6. Castiblanco, F., Oviedo Regueros, L.A.: Computer risk analysis and suggestion of controls for risk mitigation using ISO/IEC 27001, 27002 and 27005 standards. Undergraduate thesis, UNAD, Bogotá, Colombia (2017). Last accessed: 25-11-2025. <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2660/Trabajo%20de%20grado.pdf>

7. NIST: NIST Cybersecurity Framework 2.0. U.S. Department of Commerce, CSWP-29, 1–32. Washington, D.C, United States of America. (2024). Last accessed: 25-11-2025. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
8. ISO: ISO/IEC 27001:2022. International Organization for Standardization. Geneva, Switzerland. (2022). Last accessed: 25-11-2025. <https://www.iso.org/es/home>
9. Dávila Fernández, M.C., Muñoz Huaman, J.: Design of cybersecurity controls to reduce cyberattacks in companies distributing digital products based on CIS Control V8. Undergraduate thesis, Peruvian University of Applied Sciences, Lima, Peru (2023). Last accessed: 25-11-2025. https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/670133/Davila_FM.pdf
10. Acevedoarango, E.A., Echeverri-Londoño, A.M.: The fat book of anilox. 2nd ed. ISBN 978-958-56544-0-2. Serviflex Arco Internacional S.A.S., Medellín, Colombia. (2017). URL only available with payment.
11. Acevedoarango, E.A.: Application of electromagnetic phenomena in the converter industry. *Mundo Eléctrico* 65, (2009). <https://www.mundoelectrico.com/edicion-n-65-20-anos>
12. Acevedoarango, E.A., Echeverri-Londoño, A.M.: The fat book of corona treatment. 3rd ed. ISBN 978-958-56544-1-9. Serviflex Arco Internacional S.A.S., Medellín, Colombia (2017). URL only available with payment.
13. Envapack.com: Graphic Establecimiento Gráfico Impresores continues to grow in the flexible packaging market with central drum flexo printers and BOBST laminating machines. (2024). Last accessed: 25-11-2025. <https://www.envapack.com/2019/05/establecimiento-grafico-impresores-continua-creciendo-en-el-mercado-de-embalaje-flexible-con-impresoras-flexo-de-tambor-central-y-maquinas-laminadoras-bobst/>
14. Hernández Sampieri, C.R., Fernández Collado, C., Baptista Lucio, P.: Research Methodology. 6th ed. McGraw-Hill, Naucalpan, Mexico (1991). Last accessed: 25-11-2025. https://apiperiodico.jalisco.gob.mx/api/sites/periodicooficial.jalisco.gob.mx/files/metodologia_de_la_investigacion_-_roberto_hernandez_sampieri.pdf
15. Casas Anguita, J., Repullo Labrador, J.R., Donado Campos, J.: The survey as a research technique. *Rev. Atención Primaria* 31(8), 527–538 (2003). Last accessed: 25-11-2025. <https://core.ac.uk/download/pdf/82245762.pdf>
16. López Giraldo, F.E.: I Seminar on Research Methodology. Training material, ITM, Medellín, Colombia. (2024). Last accessed: 06-11-2024. <https://campusvirtual.itm.edu.co/>
17. Vargas Montoya, H.F.: IV Seminar on Research Methodology Course. Training material, ITM, Medellín, Colombia. (2025). Last accessed: 13-11-2025. <https://campusvirtual.itm.edu.co/>
18. Álvarez Gaviria, S.A.: Networks and Cybersecurity Course. Training material, University of Antioquia (Sapiencia), Medellín, Colombia. (2024). Last accessed: 10-02-2024. <https://ingenia.udea.edu.co/>
19. Marín R., L.: Risk Analysis and Management Course. Training material, ITM, Medellín, Colombia. (2024). Last accessed: 14-06-2024. <https://campusvirtual.itm.edu.co/>
20. Technological Journal – ESPOL: Methodology for risk analysis and evaluation applied to computer security under the ISO/IEC 27001 standard. *Technological Journal – ESPOL* 28(5), (2015). Last accessed: 25-11-2025. <https://rte.espol.edu.ec/index.php/tecnologica/article/view/456>
21. National Cybersecurity Training & Educational Center (NCyTE Center): The McCumber Cube and CIA Triad; E-Mate 2.0 (Online animation), National Science Foundation (NSF) (2025). Last accessed: 25-11-2025. <https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad>

Marco CCCI: Estrategia pedagógica, didáctica y técnica para facilitar la comprensión de un modelo de ciberseguridad industrial basada en un proceso ingenieril de innovación mediante el mejoramiento del cubo de McCumber

ICTBC framework (CCCI): Pedagogical, didactic and technical strategy to facilitate the understanding of an industrial cybersecurity model based on an innovative engineering process by improving the McCumber cube

Edgar Alberto Acevedoarango ¹ y Adriana María Echeverri Londoño ²

Tipo de Artículo: Investigación revisión.

Recibido: 16/10/2025. Aprobado: 00/00/0000. Publicado: 00/00/0000

Resumen: El “Cubo Campanito de la Ciberseguridad Industrial” (CCCI) es un nuevo marco técnico y pedagógico para facilitar la gestión de protección cibernética. Fue creado con el objetivo de apoyar las labores de ciberdefensa en PYMEs y empresas que operan cadenas de producción críticas en sectores industriales esenciales. La creación del CCCI se efectuó mediante la aplicación de un proceso de innovación ingenieril que, expandió, complementó, actualizó, adaptó, mejoró y fortaleció el tradicional y muy conocido cubo de McCumber de la seguridad informática de los años 90 y surgió, como un desarrollo complementario y colateral, de un trabajo de investigación que se realizó como tesis de maestría en seguridad informática en el I.T.M. de Medellín.

Inicialmente, el marco CCCI se centró y se aplicó en el sector flexográfico, sin embargo, su diseño, estructura, flexibilidad metodológica, alcance y potencia didáctica, permiten adaptarlo con facilidad, como guía técnica de seguridad informática y como herramienta pedagógica, en otras industrias con similares características de criticidad en sus cadenas productivas. Esto se debe a que el CCCI facilita la comprensión, asimilación y adopción de los conceptos técnicos, actividades y funciones clave de la ciberseguridad en todos los niveles de una organización, promoviendo la protección y aseguramiento de la confidencialidad, integridad y disponibilidad de la seguridad de la información de las infraestructuras computacionales asociadas a la gestión de las cadenas de producción esenciales y difícilmente reemplazables. Complementariamente, el CCCI, por naturaleza y diseño, integra un enfoque pedagógico que ayuda a visualizar, asimilar y entender, con facilidad, los conceptos técnicos complejos de la seguridad informática, proporcionando los fundamentos y bases necesarias para una adecuada ciberdefensa en profundidad que, también, sea adaptable, efectiva y práctica para PYMEs y empresas del ámbito industrial.

Palabras clave: *Ciberseguridad industrial; Cubo de McCumber; Cubo Campanito de Ciberseguridad Industrial (CCCI); Flexografía; Infraestructuras Críticas; PYMEs.*

¹ **Edgar Alberto Acevedoarango:** Ingeniero Eléctrico (U. Nacional de Colombia, Facultad Nacional de Minas, Medellín); Magister en Administración de Empresas, M.B.A. (U. EAFIT); Especialista en Negocios Internacionales (U. EAFIT); Especialista en Ciberseguridad (I.T.M.); Magister en Seguridad Informática (c) (I.T.M.); Especialista en Analítica de Datos (c) (Politécnico Colombiano Jaime Isaza Cadavid). I.T.M. / Politécnico Colombiano Jaime Isaza Cadavid. Gerente de Innovación, Proyectos, I+D y nuevas tecnologías (Serviflex Arco USA LLC, Redondo Beach, CA, Estados Unidos de América y Serviflex Arco Internacional S.A.S., Medellín, Ant., Colombia). eaa.researcher@gmail.com; ORCID: <https://orcid.org/0009-0001-1339-0517>. Medellín, Colombia.

² **Adriana María Echeverri Londoño:** Ingeniera Química (Universidad de Antioquia, Facultad de Ingeniería); Magister en Administración, M.B.A. (Universidad EAFIT); Especialista en Gerencia de la Calidad (Universidad EAFIT); Especialista en Ciberseguridad (I.T.M.); Magister en Seguridad Informática (c) (I.T.M.); I.T.M. Gerente Técnica y de Seguridad Informática (Serviflex Arco USA LLC, Redondo Beach, CA, Estados Unidos de América y Serviflex Arco Internacional S.A.S., Medellín, Ant., Colombia). ameltempo1212@gmail.com; ORCID: <https://orcid.org/0009-0002-4525-076X>. Medellín, Colombia.

Abstract. *The Industrial Cybersecurity Tinker Bell Cube, ICTBC (CCCI in spanish) is a new technical and pedagogical framework to facilitate cybersecurity management. It was created to support cyber defense efforts in SMEs and companies operating critical production chains in essential industrial sectors. The ICTBC was developed through an engineering innovation process that expanded, complemented, updated, adapted, improved, and strengthened the traditional and well-known McCumber Cube for computer security from the 1990s. It emerged as a complementary and collateral development from research conducted as a master's thesis in computer security at the ITM in Medellín.*

Initially, the ICTBC framework was focused on and applied to the flexographic printing sector. However, its design, structure, methodological flexibility, scope, and didactic power allow it to be easily adapted, both as a technical guide to cybersecurity and as a pedagogical tool, to other industries with similar criticality characteristics in their production chains. This is because the ICTBC facilitates the understanding, assimilation, and adoption of key cybersecurity technical concepts, activities, and functions at all levels of an organization, promoting the protection and assurance of confidentiality, integrity and availability of information security for the computing infrastructures associated with the management of essential and irreplaceable production chains. Additionally, the ICTBC, by its very nature and design, integrates a pedagogical approach that helps to easily visualize, assimilate, and understand complex technical concepts of cybersecurity, providing the necessary foundations and basis for adequate cyber defense in depth that is also adaptable, effective, and practical for SMEs and companies in the industrial sector.

Keywords: *Critical Infrastructure; Flexography; Industrial cybersecurity; Industrial Cybersecurity Tinker Bell Cube (ICTBC); McCumber Cube; SMEs.*

I. Introducción y planteamiento del problema

Introducción

La creación del marco CCCI se deriva de un trabajo de investigación desarrollado como tesis de maestría en seguridad informática (Acevedoarango y Echeverri L, 2025a) [1] en I.T.M. e introduce un proceso ingenieril de innovación, que implementa la expansión, adaptación, complementación, fortalecimiento, mejoramiento y actualización del conocido cubo McCumber de la seguridad informática (McCumber, 1991) [2]. Dicho nuevo marco, CCCI, surge de la necesidad de visibilizar, facilitar la comprensión y el entendimiento y, también, de promover la adopción e implementación de un modelo de ciberseguridad en la industria flexográfica, particularmente en PYMEs con cadenas de producción esenciales, críticas y difícilmente remplazables.

En efecto, la transformación digital ha generado profundos cambios en los procesos productivos e industriales, como se infiere del trabajo de (Brito y Díaz, 2023) [3]. Al respecto y según se infiere de (Mejía, 2024) [4], en sectores como el flexográfico, encargado de producir envases, etiquetas y embalajes para industrias esenciales, esta evolución ha implicado la incorporación progresiva de tecnologías como la informática, la automatización, incluso los sistemas de control digital (DCS) como los estudiados por (Acevedoarango, 1996) [5]. Además, el internet de las cosas (IoT) y, más recientemente, la inteligencia artificial (IA) han arribado con fuerza y gran penetración a los sectores productivos industriales. Si bien estos avances han mejorado la productividad, también, han aumentado y agravado significativamente la exposición al riesgo cibernético de las industrias, especialmente, en las PYME, las cuales, a menudo carecen de estrategias de seguridad digital, formalmente implementadas, como afirma (Castiblanco y Oviedo, 2017) [6].

En este sentido, el objetivo del Cubo Campanito de Ciberseguridad Industrial (CCCI) (Acevedoarango y Echeverri L, 2025a) [1], surgió como un resultado colateral e inesperado del trabajo de desarrollo de un modelo de ciberseguridad sectorial, estableciéndose como marco de estrategia pedagógica y técnica, para facilitar la comprensión, apropiación e implementación de los modelos de ciberseguridad industrial. Es importante resaltar que, aun cuando el CCCI nació de una investigación específica en la industria colombiana de impresión flexográfica, al igual que su antecesor, el cubo de McCumber, en realidad se trata de un marco de seguridad informática de ámbito universal y potencialmente aplicable a otros sectores industriales similares con cadenas productivas críticas. El marco CCCI propuesto se basa en el reconocimiento de un desafío industrial común: la complejidad técnica de los

modelos de seguridad de la información y su limitada comprensión por parte de gerentes, directores y personal no especializado en ciberseguridad, lo que limita su potencial de adopción y aplicación organizacional.

Para superar este obstáculo, se diseñó el marco CCCI, una estrategia de visualización de modelos de ciberseguridad industrial, basada en fundamentos pedagógicos y didácticos, articulada a través de un proceso de innovación ingenieril, que dio como resultado la mejora conceptual del cubo McCumber de seguridad informática, propuesto hace más de tres décadas, en 1991, por el Ing. John R. McCumber, en un evento de la NCSC (McCumber, 1991) [2].

Se trata de un marco clásico de protección de la seguridad de la información ampliamente reconocido en el ámbito de las empresas y organizaciones. La propuesta consistió en actualizar y complementar el cubo original, ampliando sus dimensiones para representar y visualizar de forma clara y completa todos los componentes de un modelo de ciberseguridad industrial. Esta nueva versión se denominó Cubo Campanito de Ciberseguridad Industrial, CCCI, y fue concebida como una herramienta educativa y técnica para facilitar la comprensión y adopción de un modelo específico de ciberseguridad corporativo entre gerentes, partes interesadas, directores senior y personal no especializado, en particular, empleados de operación y personal lego en la materia.

El desarrollo del CCCI surge de un enfoque investigativo que integró principios de ingeniería de procesos, seguridad de la información, pedagogía, didáctica e innovación conceptual, con el propósito de crear una solución comprensible, aplicable y replicable para la concientización, capacitación y toma de decisiones estratégicas en entornos de ciberseguridad industrial; traduciendo la complejidad técnica a un lenguaje accesible para personal no especializado y aportando valor técnico en contextos reales (Acevedoarango y Echeverri L, 2025a) [1].

Su diseño ingenieril garantiza alineación con estándares internacionales como NIST CSF 2.0 (NIST, 2024) [7], ISO 27001 (ISO/IEC, 2022) [8] y CIS Controls (Dávila y Muñoz, 2023) [9], así como con buenas prácticas de ciberseguridad, lo que le permite enfrentar eficazmente los riesgos cibernéticos actuales. Consolidado como recurso técnico y pedagógico, el CCCI fortalece la resiliencia digital, la continuidad operativa y la sostenibilidad organizacional en sectores con infraestructura crítica, posicionándose como una propuesta de innovación educativa y de ingeniería aplicada que facilita la adopción de estrategias complejas entre personal no técnico, y establece las

bases para su adaptación en otros sectores productivos clave para la economía real.

Planteamiento del problema

La industria flexográfica, como consignan (*Mejía, 2024*) [4], (*Acevedoarango y Echeverri L., 2017a*) [10], (*Quintana, Cornejo y Rigail, 2007*) [14], al igual que otras industrias esenciales con cadenas de producción críticas, constituye un pilar fundamental de la economía real, pues, sus productos son utilizados en la cadena logística y de suministro de otras industrias igualmente críticas y difícilmente remplazables en el corto plazo.

Complementariamente, y como se consigna en (*Acevedoarango y Echeverri L., 2025a*) [1], la creciente digitalización de los procesos industriales y la interconexión de los sistemas productivos al ciberespacio, han expuesto a los sistemas IT que operan y gestionan las cadenas productivas de las empresas, especialmente a las PYMEs, ante una amplia gama de amenazas cibernéticas. Esto en razón a la característica falta de recursos técnicos, financieros y humanos dedicados a la seguridad informática en dicho nicho empresarial. Como consecuencia, la vulnerabilidad de las cadenas productivas críticas del sector flexográfico, así como las de otras industrias esenciales, representa en la actualidad, un riesgo significativo para la continuidad operativa, la resiliencia productiva y la competitividad de las compañías de los diversos sectores industriales, lo cual se traduce en un riesgo potencial para la economía real, la sociedad, el país, e incluso el mundo entero.

De esta manera, la necesidad de protección y preservación del rol y operación de industrias como la flexográfica es vital e irremplazable, pues contribuyen con otras industrias, igualmente críticas e insustituibles para la sociedad, como son la industria alimentaria, la farmacéutica, de bienes y productos de primera necesidad, entre muchas otras. Adicionalmente, industrias, como la flexográfica, se enfrentan a desafíos de seguridad informática cada vez mayores, debido a la proliferación, crecimiento exponencial, diversificación y sofisticación de las amenazas cibernéticas.

De otra parte, en la industria flexográfica, al igual que en otros sectores productivos, propender por el aseguramiento de la continuidad operacional y la resiliencia de la infraestructura informática asociada a la gestión de las cadenas productivas esenciales constituye un aspecto crítico para la estabilidad de la producción y para la sobrevivencia de las empresas, en particular, si se trata de PYMEs, cuya caracterización comienza por limitación de recursos para inversión en tecnología, escasez de personal calificado en ciberseguridad, desconocimiento y poco o nulo entendimiento, a nivel organizacional, de la dimensión

técnica de la seguridad informática, en especial, por parte de la alta directiva, pero, también, de funcionarios del común y, en especial de los empleados de planta y el personal de producción. En este contexto, cobra especial importancia el rol del nuevo marco CCCI, como herramienta pedagógica y de orientación técnica, como se verá en mayor detalle más adelante.

Desde esta perspectiva, como bien afirman (*Acevedoarango y Echeverri L., 2025a*) [1], la continuidad operacional en entornos industriales, como el flexográfico, implica la implementación de una estrategia de seguridad informática que permita mantener las operaciones y la producción sin colapsar, no solo ante ciberataques, sino, también, ante incidentes imprevistos, como fallas tecnológicas, contingencias, calamidades naturales o desastres de cualquier índole.

Por tanto, se encontró que la adopción de un enfoque de protección cibernética basada en la gestión de riesgos, como plantean (*Bríto y Díaz, 2023*) [3] y (*Castiblanco y Oviedo, 2017*) [6], pero, sobremanera, la adopción de las premisas y recomendaciones de estándares internacionales, como el marco NIST 2.0 CSF (*NIST, 2024*) [7], la norma ISO 27001 (*ISO/IEC, 2022*) [8], los CIS Controls (*Dávila y Muñoz, 2023*) [9], las normas ISO 22301, ISO 22361, ISO 22316 (*Acevedoarango y Echeverri L., 2025a*) [1] entre otros estándares y referentes, resultan, al final del día, de esencial importancia, permitiendo a las compañías, la rápida y oportuna identificación de vulnerabilidades, así como el establecimiento de mecanismos prácticos y adaptables de respuesta a incidentes o ciberataques, que, sobre manera, sean efectivos y eficaces en su nivel de protección de las infraestructuras IT.

Finalmente, todas estas necesidades de protección cibernética se consolidan en la urgencia de implementar modelos de ciberseguridad en las industrias; modelos de seguridad informática, normalmente complejos a la luz de lo técnico y de difícil comprensión, entendimiento y asimilación por parte de personal no especializado de las organizaciones (incluyendo gerentes, personal administrativo, personal de planta, operarios, et al), lo cual se traduce en una gran dificultad para la adopción de los prototipos cibernéticos de protección.

Es en este contexto donde entra a jugar el nuevo marco CCCI, por una parte, como herramienta pedagógica y didáctica de visibilización, que permite facilitar la comprensión, entendimiento y asimilación de los conceptos técnicos y de las complejidades y minucias ingenieriles de un modelo de ciberseguridad y, por otro lado, como guía técnica y directriz orientadora de la seguridad informática que requiere cada organización.

II. Marco teórico y estado del arte

Marco teórico

• Flexografía y ciberseguridad

Como se infiere de los trabajos de investigación de (Mejía, 2024) [4], (Acevedoarango y Echeverri L., 2017, a) [10], (Acevedoarango, 2009) [11] y (Acevedoarango y Echeverri L., 2017b) [12], la industria flexográfica es un sector clave de la economía real que se dedica a la producción de empaques flexibles y rígidos, cajas, etiquetas, envases, contenedores y embalajes, todos ellos, productos que forman parte de las cadenas de suministro de otras industrias igualmente críticas, como la alimentaria, farmacéutica, de bienes y necesidades.

Según (Acevedoarango y Echeverri L., 2017a) [10], esta industria se caracteriza por el uso del Anilox (rodillo grabado con microceldas, utilizado para transferir la tinta al sustrato que se imprime) y, también, por otros procesos descritos con más detalle por (Mejía, 2024) [4], (Acevedoarango y Echeverri L., 2017a) [10], (Acevedoarango, 2009) [11] y (Acevedoarango y Echeverri L., 2017b) [12], lo cual, hoy en día, hace de la flexografía, una industria floreciente y necesaria para la sociedad y la economía real, debido a su naturaleza neurálgica y esencial, demostrada por la pasada pandemia de Covid-19, que puso de manifiesto su condición de infraestructura productiva crítica. La Figura 1 muestra una cadena de producción típica de la industria flexográfica.

Figura 1. Cadena productiva crítica típica de la industria flexográfica (Planta). **Fuente:** Tomado de (Envapack.com, 2024) [13].



Nota. Vista de una planta típica de producción flexográfica actual con su cadena productiva crítica. **Fuente:** Tomado de (Envapack.com, 2024) [13].

En este contexto, como cadena industrial de producción esencial y compleja de sustituir o reemplazar,

en el corto plazo, el sector flexográfico se enfrenta a crecientes amenazas cibernéticas debido a la digitalización e incorporación de tecnologías como la inteligencia artificial (IA), el internet de las cosas (IoT), los sistemas de control digital (SCD), la robótica, los sistemas de control numérico (SCN), entre muchos otros, que convierten su cadena de producción, en un proceso crítico, cuya superficie de exposición está altamente desvelada y vulnerable ante ciberataques, precisamente, en razón a su alto nivel de automatización con tecnologías de punta, general y permanentemente, conectadas al ciberespacio.

• Infraestructuras de producción críticas.

Por otra parte, y según fuentes citadas en (Acevedoarango y Echeverri L., 2025a) [1], el sector flexográfico es una parte fundamental del sector real de la economía y sus procesos, infraestructura y equipamiento productivo son considerados prioritarios y esenciales desde la pasada pandemia de Covid-19, aun cuando no están formalmente incluidos dentro de la definición estatal de infraestructura crítica.

Dicho sector industrial, como se infiere en (Mejía, 2024) [4] y en (Quintana, Cornejo y Rigail, 2007) [14], incluye las industrias de la flexografía o de impresión flexográfica, siendo un sector especializado en la producción de empaques, etiquetas, cajas de cartón corrugado, envases y embalajes impresos, todos los cuales son productos primordiales, insustituibles e irremplazables en las cadenas logísticas que, igualmente y de manera similar a la industria flexográfica, cuentan con infraestructuras productivas tan críticas como esenciales y que pertenecen a otras ramas industriales como, por ejemplo, las industrias alimentaria, la farmacéutica, la de bienes, productos y mercancías básicas y de primera necesidad, entre muchas otras más.

En este punto es importante enfatizar que otro aporte del trabajo de investigación de (Acevedoarango y Echeverri L., 2025a) [1], es robustecer la diferenciación entre la tradicional concepción de infraestructuras críticas y las infraestructuras productivas críticas, que son más propias de la industria real y que están destinadas, como su nombre indica, específicamente a las labores de producción en el contexto de la economía real.

• El “Cubo de MacCumber de la Seguridad Informática”

El conocido “Cubo de MacCumber de la Seguridad Informática”, según se observa de (Acevedoarango y Echeverri L., 2025a) [1] y de (McCumber, 1991) [2], fue una idea propuesta durante la celebración de la 14ava Conferencia Nacional de Seguridad Computacional de los Estados Unidos (14th National Computer Security

Conference, NCSC - NSA, Washington DC; 1991). Dicha creación fue ideada y propuesta por el ingeniero americano John R. McCumber (ver Figura 2, siguiente), Capitán (*retirado*) de la Fuerza Aérea de los Estados Unidos (U.S.A.F.), quién, además, estuvo adscrito a las fuerzas de inteligencia del Pentágono y quién, también, se desempeñó como analista de seguridad de la Agencia de Seguridad Nacional de los Estados Unidos (*National Security Agency, N.S.A.*).

En este contexto, McCumber, inspirado en un discurso de Michelle Van Cleave (*abogada experta en política de seguridad, defensa e inteligencia y primera mujer en ocupar el cargo estatutario de Office of the National Counterintelligence Executive (NCIX) de la Office of the Director of National Intelligence (ODNI) de los Estados Unidos*), realizada durante el año inmediatamente anterior, en el escenario del 13th *National Computer Security Conference (NCSC - NSA, Washington DC; Estados Unidos, 1990)* y en la cual, dicha funcionaria, manifestaba la importancia, necesidad y urgencia de desarrollar una estructura conceptual o marco de seguridad informática de fácil entendimiento, que hiciera visibles, entendibles y prácticos los conceptos complejos de la ciberseguridad.

Figura 2. Ing. John R. MacCumber. **Fuente:** Tomado de (*RSA Conference, 2016*) [15].



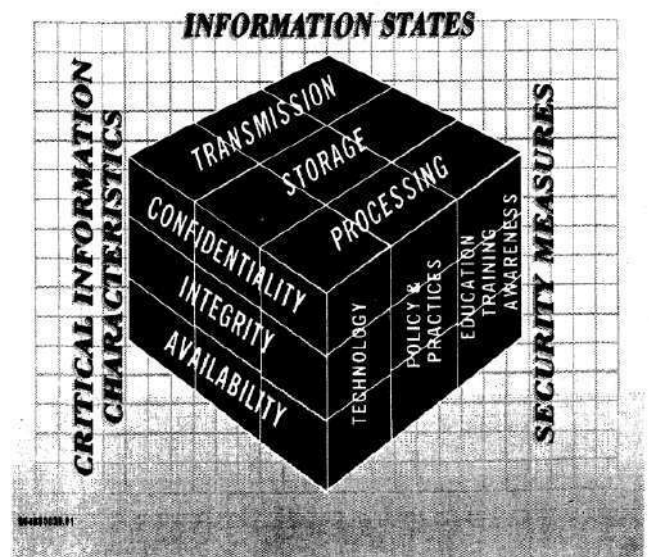
Nota. Imagen de J.R. McCumber en 2016 durante la RSAC. **Fuente:** Tomado de (*RSA Conference, 2016*) [15].

Así pues, McCumber puso manos a la obra e ideó su conocido constructo de ciberseguridad (ver Figura 3, más adelante), el cual terminó siendo más conocido como el “Cubo de McCumber de la Seguridad Informática”. Las dimensiones originalmente propuestas por McCumber fueron: Dimensión de los objetivos de la Seguridad, dimensión de los Estados de la Información y dimensión de los Mecanismos de Seguridad Informática. Consecuentemente, dicho marco conceptual, técnico metodológico y, por supuesto, también, pedagógico, fue formalizado, oficializado y presentado en sociedad, en su ponencia intitulada: “*Information systems security: a comprehensive model*”

durante la conferencia nacional de computación, a principios de la década de los 90 (*NCSA - NSA, Washington, 1991*).

En dicha conferencia, basándose en su gran experiencia y amplio conocimiento técnico en ciberseguridad e, inspirado, también, en el conocido y mundialmente famoso “Cubo Mágico” o “Cubo Rubik” (*desarrollado por el arquitecto y escultor húngaro Erno Rubik en 1974*), McCumber consolidó su marco integral y conceptual de seguridad informática, el cual ha perdurado hasta la actualidad.

Figura 3. Cubo de McCumber de la seguridad informática (*imagen original de la ponencia de la NCSA de 1991*). **Fuente:** Tomado de (*McCumber, 1991*) [2].



Nota. Basado en el cubo mágico o cubo Rubik, el marco tradicional de McCumber propone tres dimensiones (*Características críticas de la información, Estados de la Información y Mecanismos de seguridad*) **Fuente:** Tomado de (*McCumber, 1991*) [2].

Al efecto, el Cubo de MacCumber de la seguridad informática se difundió rápidamente en el ámbito de la seguridad informática americana y mundial, popularizándose durante el periodo la década de los 90, pero, particularmente en eventos especializados entre 1991 y 1992, como se infiere de las reseñas incluidas y citadas en (*Acevedoarango y Echeverri L, 2025a*) [1] y que se puede consultar, también, en las memorias de dicha conferencia nacional de seguridad computacional (ver (*McCumber, 1991*) [2]). Información adicional sobre el cubo de McCumber de la Seguridad Informática puede encontrarse en (*Maconachy, Schou, Ragsdale y Welch, 2001*) [16].

A pesar de constituir una referencia clásica atemporal, el aporte de McCumber adolece, en la actualidad, de falencias derivadas de la exposición al riesgo, ocasionadas por los avances tecnológicos en muy diversos campos, quedándose ya corto, ante los

requerimientos de protección cibernética que requieren los sistemas IT hoy día, en particular, de aquellos asociados a infraestructuras críticas de naturaleza industrial. De otra parte, también, es menester reconocer que sus fundamentos, aún constituyen cimiento valioso e indiscutible de la labor de defensa informática.

Estado del arte

Respecto, al estado del arte, como se consigna en (Acevedoarango y Echeverri L, 2025a) [1], se encuentran multitud de trabajos e investigaciones, tanto a nivel de pregrado, como de postgrado (incluidas maestrías y doctorados) sobre diversas modalidades y formatos de modelos y prototipos de ciberseguridad; todos ellos aplicados a los más diversos sectores, como, por ejemplo, empresas de servicios tecnológicos, empresas del sector energético, compañías del sector financiero y bancario, entidades cooperativas, instituciones públicas, instituciones educativas, organizaciones privadas vinculadas a la moda, el sector turismo, el sector alimentario, el sector textil, entre muchas otras.

Sin embargo, en todas ellas, en general, se encontró que la labor de investigación se circunscribió a solucionar cada caso individual, acorde a los requerimientos técnicos específicos de cada requerimiento de ciberseguridad organización, ya se tratase de compañías privadas o de instituciones del sector público. Así se obtuvo una amplia gama de soluciones que presentan diversas metodologías y métodos individuales y particulares.

Con la introducción del nuevo marco CCCI, se espera aportar un valor agregado diferenciador al área de la ciberseguridad, retomando y mejorando un marco tradicional, como lo es el “Cubo de McCumber de la Seguridad Informática” y reacondicionándolo, a través de un proceso ingenieril de innovación, que implicó, adecuarlo, fortalecerlo, adaptarlo, extenderlo y actualizarlo a las necesidades de protección cibernética de las infraestructuras informáticas asociadas a la gestión de las cadenas producción críticas de diversos sectores de la industria real de nuestros días.

III. Materiales, métodos y metodología de investigación

Materiales

La metodología de investigación implementada para el diseño del modelo de ciberseguridad buscado, se basó en indicaciones de (López, 2024) [17] sobre la aplicación del método científico, que fue desarrollado bajo el esquema paso a paso (*Step by step*) y acorde a los lineamientos sugeridos por (Hernández, Fernández y Baptista, 1991) [18], lo cual, incluyó, la aplicación de dos instrumentos (*Diagnóstico, durante la fase 1 y*

Validación, en la fase 3) según las recomendaciones de (Casas, Repullo y Donado, 2003) [19].

Este derrotero, que sirvió como una guía metodológica estructurada y rigurosa, direccionó el proceso de indagación, de revisión bibliográfica y de la labor de investigación, en general. Así pues, se consultaron diversas fuentes de información, principalmente los repositorios de universidades públicas y privadas locales y algunas internacionales. Se analizaron varios artículos de investigación, muchos a nivel de maestría y algunos incluso de doctorado. Luego, el método se aplicó fase por fase, tal como se muestra en la Figura 4 (Ver Figura 4), implementándose el prototipo cibernético de protección (*basado en la revisión y extracción de controles de ciberseguridad derivados de los estándares internacionales ya referidos (Marco NIST 2.0 CSF (NIST, 2024) [7], norma ISO 27001 (ISO/IEC, 2022) [8] y los CIS Controls (Dávila y Muñoz, 2023) [9]).*

Métodos y metodología de investigación

El diseño del modelo de ciberseguridad para la industria flexográfica se consolidó mediante el desarrollo de una metodología por fases (*step by step*). Para ello, se estructuraron varias etapas de investigación sucesivas y articuladas, con actividades y subactividades, que permitieron la recolección secuencial, gradual y oportuna de resultados.

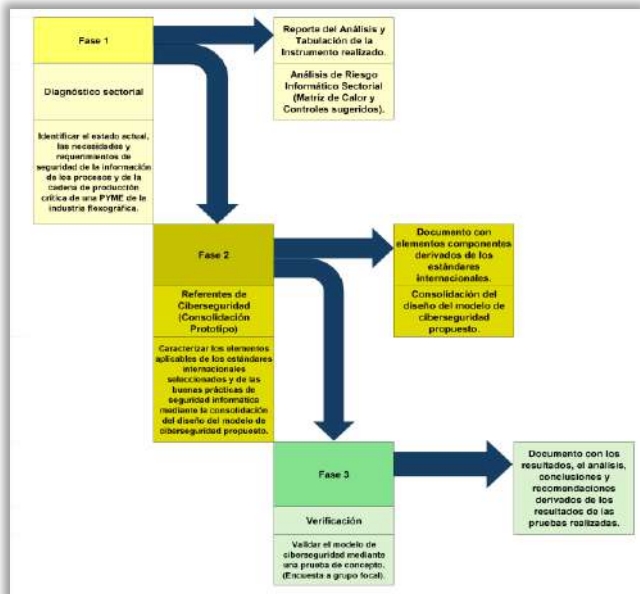
De esta manera, los logros investigativos se consolidaron en tres fases principales: *fase 1* de diagnóstico sectorial del estado y necesidades de seguridad de la Información sectorial; *fase 2* de análisis de estándares y referentes internacionales de seguridad informática y consolidación del prototipo de ciberseguridad, lo cual significa, en la práctica, la selección adecuada e idónea de controles informáticos derivados de los tres referentes y estándares utilizados (*marco NIST 2.0 CSF (NIST, 2024) [7], norma ISO 27001 (ISO/IEC, 2022) [8] y los CIS Controls (Dávila y Muñoz, 2023) [9]*), y; *fase 3* de validación del modelo a través de un instrumento metodológico aplicado a un grupo focal de expertos.

En este punto, es menester mencionar que, la fase de validación y verificación se realizó sobre el objetivo de la tesis de maestría, el cual es el modelo de ciberseguridad para el sector flexográfico y no para el marco CCCI propiamente dicho, que finalmente, resultó como valor agregado de la investigación.

Sin embargo, a tal propósito, se utilizó el marco CCCI para introducir y explicar el modelo de ciberseguridad desarrollado a las diversas organizaciones de la industria flexográfica con gran éxito, pues permitió hacer más fácil el entendimiento del prototipo de protección cibernética y la asimilación de los conceptos técnicos de

ciberseguridad, tanto por parte de las altas directivas, como de personal de planta y de operación, traducándose en una entusiasta recepción sectorial para su futura adopción.

Figura 4. Fases metodológicas de la investigación que condujo a la creación del nuevo marco CCCI. **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. Autoría propia.



Nota. En contexto de la metodología aplicada, el nuevo marco CCCI surgió en la fase de desarrollo del prototipo cibernético de protección, como solución a la necesidad didáctica y técnica de visibilizar y lograr una buena comprensión del modelo propuesto para su adopción en la industria, pero, fue consolidado en la fase de validación y verificación del modelo de ciberseguridad, a través de un instrumento metodológico (encuesta a focus group). **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. Autoría propia.

En este contexto, fue precisamente que, se observó la dificultad cognitiva derivada de dos factores trascendentales de este tipo de tesis de maestría en seguridad informática: la definición de “modelo”, que puede enunciarse, casi literalmente, como: “estructura conceptual de carácter y naturaleza abstracta”; a lo que se puede agregar el obstáculo epistemológico que representaba la natural complejidad técnica del modelo de ciberseguridad para cualquier lego en la materia, particularmente, para el personal operativo, razones por las cuales, se decidió buscar un mecanismo pedagógico y didáctico que, sin perder la potencia técnica, facilitara la comprensión de un modelo de ciberseguridad por parte de gerentes, directores, operadores y, en general, personas no especializadas en el campo de la seguridad informática y se encontró al cubo McCumber como ideal para tal fin.

En consecuencia, y como resultado, el marco de ciberseguridad CCCI fue concebido y creado como resultado indirecto y como el más relevante valor agregado de (Acevedoarango y Echeverri L, 2025a) [1]. En

general, esta metodología permitió el desarrollo de un modelo de ciberseguridad adaptable y contextualizado que es técnicamente robusto, eficiente y efectivo, y, lo que es más importante, pedagógicamente comprensible y técnicamente sólido, acorde con los preceptos aprendidos de (Vargas, 2025) [20], (Álvarez, 2024) [21], (Marín, 2024) [22] y (ESPOL, 2015) [23].

Así, a través de una estrategia de innovación realizada mediante un proceso de ingeniería, el marco CCCI que fundamentó y visibilizó el modelo de ciberseguridad para la industria en estudio, generó un claro beneficio adicional, no solo basado en su fundamento técnico de naturaleza cibernética, que opera bajo estándares internacionales, sino, también, por la facilidad que posibilitó para la asimilación de las gerencias y altos directivos de las organizaciones, lo cual conduce a su adaptación práctica a la realidad industrial del sector objetivo. En otras palabras, a través de un proceso de innovación conceptual de carácter ingenieril, el CCCI, logra “vender la idea de la ciberseguridad y hacerla parte prioritaria y esencial de la cultura y el quehacer organizacional de la industria” robusteciendo su capacidad de continuidad operativa y resiliencia digital.

En este orden de ideas, vale destacar que, desde la perspectiva metodológica, se descubrió que el enfoque pedagógico es clave para asegurar la apropiación del CCCI, tanto por parte de las gerencias como del personal no especializado, mientras que el componente de ingeniería del marco CCCI garantiza su solidez técnica y su alta capacidad de protección y ciberdefensa en profundidad. De otra parte, se espera que la validación del modelo de ciberseguridad para la industria flexográfica confirme la utilidad real del CCCI como una herramienta replicable en el sector flexográfico y, también, en otros sectores industriales esenciales con características similares en sus infraestructuras críticas de producción y con necesidades de protección y ciberdefensa parecidas.

IV. Resultados

Marco CCCI: Cubo Campanito de Ciberseguridad Industrial.

• Presentación general del CCCI

El desarrollo del CCCI constituye un resultado obtenido importante en el área de la ciberseguridad, pues en esencia, el nuevo marco “Cubo de Campanito de Ciberseguridad Industrial” (*Industrial Cybersecurity Tinker Bell Cube, ICTBC, en inglés*), surgió como resultado de la aplicación de un proceso ingenieril de innovación, producto de la labor de investigación realizada y cuyo objetivo principal fue abordar los desafíos de ciberseguridad específicos de la industria flexográfica.

Respecto a la creación del CCCI, debe tomarse en consideración, que la industria flexográfica, al igual que muchas otras industrias de la economía real, a nivel nacional y mundial, que poseen cadenas de producción críticas, se trata de un sector productivo esencial caracterizado por una alta dependencia tecnológica y una creciente exposición a riesgos cibernéticos, especialmente en el segmento de PYMEs, según se consigna en (Acevedoarango y Echeverri L, 2025a) [1] y se revela del material formativo de (Vargas, 2025) [20], (Álvarez, 2024) [21], (Marín, 2024) [22] y (ESPOL, 2015) [23], razón por la cual la necesidad de un modelo cibernético protectivo es esencial.

En este propósito, el proceso de investigación identificó una brecha epistemológica entre el diseño tradicional de modelos de seguridad cibernética y su aplicabilidad en entornos industriales reales. Esto motivó la conceptualización de una herramienta pedagógica y didáctica que integrará principios de ingeniería, conceptos técnicos de ciberseguridad y visualización estratégica, cuya potencia fuese, también, extensible a todo tipo de industrias con infraestructuras productivas críticas. Esto derivó en la creación del CCCI como proceso de mejora y actualización del cubo de McCumber.

En este punto, también es muy importante resaltar que, luego de considerar los requerimientos de diseños previos disponibles en otros trabajos de investigación y ante la necesidad de proponer un marco estructural y conceptual que permitiera la visibilidad, fácil entendimiento y comprensión y, sobre todo, la implementación, aterrizamiento y visibilización del modelo de ciberseguridad desarrollado, se ideó el nuevo marco CCCI.

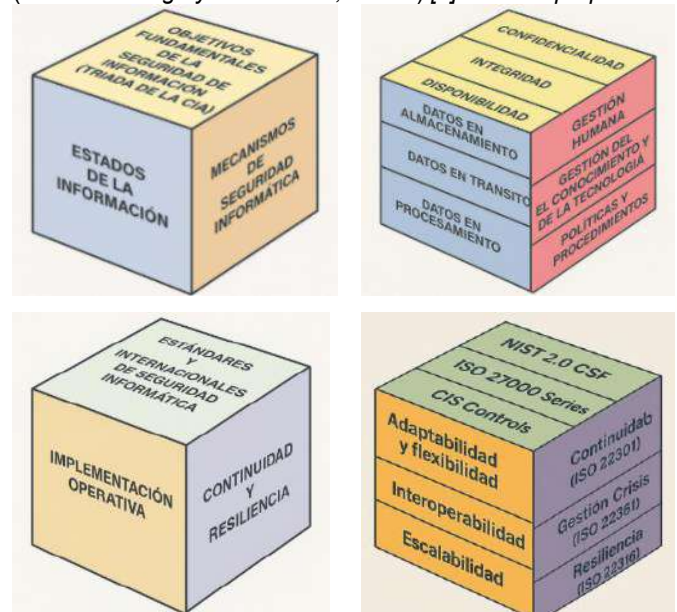
• Constitución del nuevo marco CCCI

Para ello, y con la finalidad de lograr una cibercobertura y una defensa a profundidad mucho más completa y robusta, acorde con las circunstancias actuales de digitalización industrial y, en particular, de los sectores productivos críticos de la economía real, se consideró necesario complementar, mejorar y actualizar, las tres dimensiones propuestas originalmente por McCumber en su constructo conceptual de 1991, mejor conocido como “Cubo de McCumber de la Seguridad Informática”, ampliando y extendiendo las capacidades de protección digital, en un nuevo y mejorado cubo de seguridad informática, específicamente orientado a las industrias esenciales: el CCCI. El “Cubo Campanito de la Ciberseguridad Industrial” (CCCI) se muestra más adelante en la Figura 5.

El nuevo marco CCCI se presenta, a continuación, en la Figura 5 y, en ella, se observa, su construcción general y su disposición de niveles dimensionales cada uno con sus respectivas subcategorías. Posteriormente,

se presenta una explicación técnica, completa y detallada, de cada dimensión y de cada subcategoría dimensional del CCCI.

Figura 5. Nuevo marco del Cubo de Campanito de Ciberseguridad Industrial (CCCI): **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. Autoría propia.



Nota. Extensión, adaptación, actualización y mejoramiento del cubo de McCumber con enfoque en sectores industriales esenciales con infraestructuras de producción críticas. El CCCI está compuesto por todos los cubos de la imagen, incluida la contribución original de McCumber. **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. Autoría propia.

Las tres nuevas dimensiones adicionales incorporadas al nuevo CCCI (*estándares y referentes internacionales de seguridad informática; implementación operativa y continuidad y resiliencia*), fueron el resultado de considerar las particularidades de las industrias esenciales de la economía real con cadenas productivas críticas.

En efecto, en este tipo de industrias, y sobremanera en sus PYMEs con limitados recursos para inversión en soluciones tecnológicas y escasez de personal especializado en ciberseguridad, la superficie de exposición al riesgo cibernético aumenta cada día, en razón a las tendencias en las ciberamenazas emergentes que reúnen alto grado de sofisticación, una mayor complejidad técnica, creciente aumento en la cantidad y la frecuencia de los ciberataques.

Las tres nuevas dimensiones adicionales incorporadas en el nuevo marco CCCI, ayudan a mitigar el riesgo digital, emergente y residual, en una infraestructura informática, incluyendo la protección ante ciberataques basados en ingeniería social, o generados con herramientas automatizadas implementadas con inteligencia artificial (IA), ayudando a defender y

combatir, tanto intentos maliciosos incipientes, como también, amenazas emergentes.

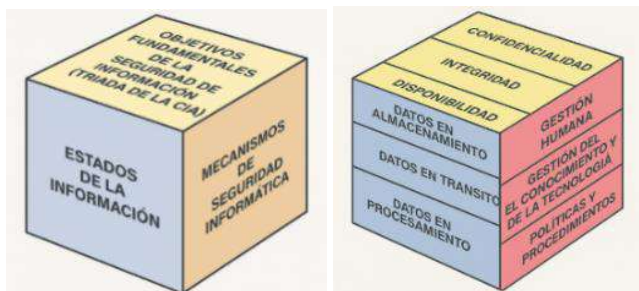
El CCCI representa un escudo ante surgimiento y establecimiento de una billonaria industria de cibercrimen organizado, como, también, el *modus procedendi* de ciberdelincuentes, especializados en cibercrimen, ciberterrorismo y ciberguerra, cuyo accionar malicioso es significativamente peligroso, pues se trata de verdaderos profesionales, altamente entrenados y tecnológicamente avanzados en conocimiento técnico y que, adicionalmente, cuentan con grandes recursos, ya propios de sus organizaciones maliciosas, o cuya fuente es un fuerte e irrestricto patrocinio estatal (*Generalmente, de países como Rusia, Corea del Norte, Irán, China, et al, cuya característica principal es una ideología opuesta a la occidental y unas fuertes dictaduras gubernamentales*).

De otra parte, el nuevo marco CCCI está conformado por las tres dimensiones originales creadas por McCumber, a lo cual, se agregan tres nuevas dimensiones ideadas por (Acevedoarango y Echeverri L, 2025) [1] y que están orientadas a fortalecer la protección cibernética industrial actual de las infraestructuras informáticas asociadas a la gestión de las cadenas productivas críticas (vale hacer notar que, el potencial de defensa en profundidad, que ofrece el CCCI, puede extenderse a muchos otros sectores fuera de la economía real).

Así pues, el CCCI está parcialmente compuesto por las tres dimensiones originales del constructo de (McCumber, 1991) [2], mostradas, a continuación, en la Figura 6, y que, a saber, son:

1. Objetivos de Seguridad
2. Estados de la Información, y
3. Mecanismos de Seguridad Informática.

Figura 6. “Cubo de McCumber de Seguridad Informática”
Fuente: Tomado de (Acevedoarango y Echeverri L, 2025a) [1].
Autoría propia.



Nota. El constructo original de McCumber está compuesto por 3 dimensiones de seguridad cibernética (Objetivos de Seguridad, Estados de la Información y Mecanismos de Ciberseguridad). La imagen presenta cada una de las subcategorías dimensionales de cada dimensión del cubo original de McCumber. **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. **Autoría propia.**

Actualmente, las dimensiones del constructo conceptual original de McCumber, presentadas en la Figura 6, aún se mantienen vigentes como un reconocido pilar de la ciberseguridad. Sin embargo, también, es necesario reconocer que, ante la complejidad, sofisticación, automatización y crecimiento exponencial de las ciberamenazas y ante actores maliciosos supremamente organizados y con infraestructuras robustas y de última tecnología, que incluso utilizan herramientas de inteligencia artificial (IA), el constructo conceptual original de McCumber se encuentra superado y ya no es un marco suficiente para proteger y asegurar la seguridad de la información en sistemas informáticos asociados a las cadenas de producción críticas de industrias esenciales.

Complementariamente, a las dimensiones anteriores se agregan, consolidando totalmente un nuevo cubo de seguridad informática (nuevo marco CCCI), las tres nacientes y nuevas dimensiones ideadas por (Acevedoarango y Echeverri L, 2025a) [1] y presentadas, a continuación, en la Figura 7, las cuales que están orientadas al propósito de robustecer la ciberseguridad industrial de la actualidad, y que, a saber, son:

4. Estándares y referentes internacionales de amplia aceptación de ciberseguridad
5. Continuidad y Resiliencia; y
6. Implementación Operativa.

Figura 7. Nuevo marco CCCI o “Cubo de Campanito de Ciberseguridad Industrial” (ICTBC: Industrial Cybersecurity Tinker Bell Cube): **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. **Autoría propia.**



Nota. Las 3 nuevas dimensiones de seguridad cibernética agregadas para expandir y actualizar el Cubo de McCumber (Estándares y Referentes Internacionales de ciberseguridad de amplia aceptación, Continuidad y Resiliencia, e Implementación Operativa) mejoran la ciberdefensa en profundidad y la protección de la seguridad de la información en entornos industriales críticos. La imagen presenta cada una de las nuevas subcategorías dimensionales de cada nueva dimensión propuestos por el CCCI. **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. **Autoría propia.**

En aras de ilustrar, con mayor detalle técnico, cada una de las dimensiones del nuevo marco CCCI, a continuación, se presentan los aspectos de protección y aseguramiento de la seguridad de la información, de cada nueva dimensión y la descripción, *grosso modo*, de

cada una de las respectivas subcategorías de cada una de sus dimensiones protectivas:

1. Dimensión de los Objetivos de Seguridad (*Confidencialidad, Integridad, y Disponibilidad*).

Esta cara del cubo, propuesta por McCumber, define qué se debe proteger. La *confidencialidad* asegura que la información solo sea accesible para usuarios autorizados; la *integridad* garantiza que los datos no sean alterados sin permiso; y la *disponibilidad* asegura que los sistemas y la información estén accesibles cuando se necesiten.

2. Dimensión de los Estados de la Información (*Transmisión, Almacenamiento, y Procesamiento de Datos*)

Esta cara, también, ideada por McCumber, describe dónde se encuentra la información en cada momento.

La información puede estar en estado de *transmisión* mientras los datos circulan, fluyen y se envían por redes. También, puede estar *almacenamiento*, cuando se guarda en dispositivos o sistemas, y, finalmente, los datos pueden estar en *procesamiento* mientras son manipulados o utilizados por programas y aplicaciones.

3. Dimensión de los Mecanismos de Seguridad Informática (*Tecnología, Políticas y Procedimientos, y Factor Humano*)

Esta cara define cómo se protege la información con mecanismos específicos como salvaguardas y controles de ciberseguridad. McCumber planteó que las *tecnologías* incluyen herramientas y sistemas de seguridad necesarios para la operación y la ciberprotección; mientras que las *políticas* y *procedimientos* establecen las directrices, lineamientos, normas y controles organizativos. Finalmente, McCumber destacó que el *factor humano*, en su calidad de eslabón más débil en la cadena de seguridad informática, abarcan capacitación, conducta del personal y prácticas que reducen errores o riesgos internos.

Al aporte de McCumber, descrito antes muy *grosso modo*, en el trabajo de investigación de (Acevedoarango y Echeverri L, 2025a) [1], se propuso incluir tres nuevas dimensiones para completar y actualizar el cubo original. Dichas nuevas dimensiones fueron resultado de la aplicación de la metodología de investigación mostrada en la Figura 4, la cual condujo a una solución al problema investigativo inicialmente planteado en este artículo.

Estas nuevas dimensiones adicionales se encontraron como producto de un proceso de innovación ingenieril aplicado por (Acevedoarango y Echeverri L, 2025a) [1] durante el tránsito investigativo realizado. En este punto, también vale la pena aclarar y hacer notar que, este nuevo constructo conceptual – el marco CCCI de

Seguridad Informática – surgió como un resultado colateral durante la investigación realizada, pues, el objetivo general y principal de dicho trabajo era el diseño de un modelo de ciberseguridad para la protección y el aseguramiento de la infraestructura informática asociada a la operación de la cadena productiva crítica de la industria flexográfica y que, realmente, el marco CCCI nació como herramienta de apoyo pedagógico y didáctico para visibilizar y facilitar la comprensión de los conceptos técnicos asociados al prototipo de protección cibernética desarrollado para dicho sector industrial).

En este contexto, las tres nuevas dimensiones consolidadas y propuestas por (Acevedoarango y Echeverri L, 2025a) [1] y que dan forma plena al nuevo marco CCCI, son las siguientes:

4. Estándares y referentes internacionales ampliamente aceptados (*Normas ISO 27000 series, marco NIST 2.0 CSF, y los CIS Controls*)

Esta nueva dimensión, propuesta por (Acevedoarango y Echeverri L, 2025a) [1], reúne los marcos normativos que guían la madurez de la ciberseguridad, tan necesaria por estos días, en particular para la industria y sectores esenciales.

La familia de normas ISO 27000 series (que incluyen normas como la ISO 27001, la ISO 27002, la ISO 27005 y la ISO 27035), el marco NIST CSF 2.0 (que incluye el factor de la gobernanza y funciones de seguridad como identificar, proteger, detectar, responder y recuperar) y, los CIS Controls (que incluyen los diez y ocho CIS Controls categorizados en: el grupo de controles básicos, el grupo de controles fundacionales y el grupo de controles organizacionales), proporcionan principios, controles y prácticas que permiten estructurar una gestión de seguridad de la información sólida, adecuada, coherente, sirviendo como la base normativa del nuevo enfoque de protección y ciberdefensa propuesto por el marco CCCI.

5. Continuidad y Resiliencia (*Normas ISO 22301, ISO 22361 e ISO 22316*)

Esta nueva dimensión, propuesta por (Acevedoarango y Echeverri L, 2025a) [1], define la capacidad de la organización para resistir, responder y recuperarse ante ciberataques o ante incidentes que afecten procesos industriales. Así mismo, la norma ISO 22301 establece los requisitos de continuidad del negocio, mientras que la norma ISO 22361 se encarga de gestionar eventuales crisis asignando responsabilidades y roles y asegurando los canales de comunicación. Y, de otra parte, la norma ISO 22316 propende por el fortalecimiento de la resiliencia, no solo operativa, sino, también, organizacional, asegurando que las operaciones críticas puedan mantenerse o restaurarse rápidamente tras una eventual interrupción. En otras palabras, esta dimensión propone, prepararse para lo peor, aguardando, siempre, lo mejor.

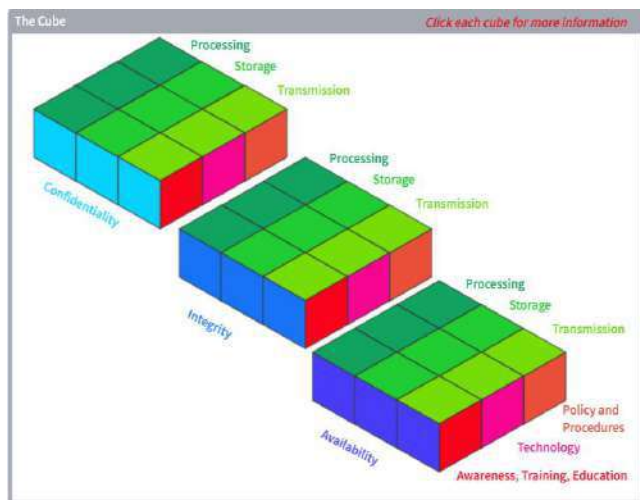
6. Implementación Operativa (*Adaptabilidad y Flexibilidad, Interoperabilidad, e Integración, y Escalabilidad*)

Esta nueva dimensión, también propuesta por (Acevedoarango y Echeverri L, 2025a) [1], para completar todas las caras de nuevo marco CCCI, describe cómo se aterriza y se construye la ciberseguridad en la operación industrial diaria, pues incluye la *adaptabilidad y flexibilidad* para responder a cambios tecnológicos, técnicos o ante ciberamenazas si fuera el caso; la *interoperabilidad e integración* permiten coordinar sistemas IT con la infraestructura OT de forma cohesiva, alineada y sincronizada; mientras que, la *escalabilidad* permite que las soluciones crezcan en la misma y justa medida del crecimiento de las organizaciones y que estas se ajusten sin comprometer la eficiencia, ni tampoco la seguridad del entorno industrial.

• Aplicación y modo de utilización del marco CCCI

Antes de continuar con la descripción de la forma en que puede ser utilizada la estructura conceptual del nuevo marco CCCI, cabe destacar que, su funcionamiento y operación son similares a los del “Cubo de McCumber de Seguridad Informática” original, ya que el mejoramiento realizado con la ampliación de tres nuevas dimensiones con sus respectivas categorías, además de extender y robustecer la idea de McCumber, complementa y actualiza el marco original de su creador.

Figura 8. Funcionamiento práctico del “Cubo de McCumber de la Seguridad Informática” y, también, del “Cubo Campanito de Ciberseguridad Industrial (CCCI)”. **Fuente:** Tomado de (NCYTE Center, 2025) [24].



Nota. Ilustración de la manera de cruzar diversas categorías dimensionales protectivas del “Cubo original de McCumber de la Seguridad Informática” y que ilustra como, en el caso del nuevo marco CCCI, las organizaciones podrían cruzar 2, 3, 4, 5 o 6 diversas categorías dimensionales de protección, acorde a sus necesidades específicas. **Fuente:** Tomado de (NCYTE Center, 2025) [24].

Esto se logró sin alterar en absoluto su concepción funcional, tanto técnica como pedagógicamente, convirtiéndola en una útil herramienta de protección cibernética. La Figura 8 muestra la intersección de las diversas subcategorías dimensionales para el “Cubo de McCumber de la Seguridad Informática” y que constituye, en esencial, el mismo *modus procedendi* para utilizar y aplicar el nuevo marco CCCI.

En otras palabras, cualquier usuario interesado puede seleccionar al menos dos de las dimensiones del nuevo marco CCCI y realizar una superposición (*utilizando el concepto de los Diagramas de Venn*) de dos o más (y hasta seis) diferentes subcategorías dimensionales, encontrando la mejor opción y los factores de protección fundamentales en el sistema informático real. Por ejemplo: confidencialidad con formación, integridad con las normas de la serie de normas ISO 27000, continuidad o resiliencia con cualquier estado de la información, etc.

Esta superposición permite interceptar, con el CCCI, hasta seis diferentes aspectos de ciberseguridad de interés para una organización. También, según se desee o se requiera, se pueden interceptar dos o más subcategorías dimensionales y así cada empresa puede ir avanzando en las especificaciones de su modelo de ciberseguridad.

En términos de ciberprotección y respecto a la seguridad informática de una organización o empresa, el funcionamiento es análogo al que se puede observar, para el constructo original de McCumber, en la animación digital tridimensional implementada en E-Mate 2.0 y disponible en el web site de (NCYTE Center, 2024) [24] y cuyos conceptos técnicos complementarios son presentados en (NCYTE Center, 2025) [25].

Modelo de ciberseguridad para la infraestructura informática asociada a la cadena de producción de la industria flexográfica

Usando y con base en el nuevo marco CCCI, se diseñó y se desarrolló un prototipo cibernético de protección para la infraestructura informática asociada a la gestión de la cadena de producción crítica de la industria flexográfica. Al efecto, se siguieron las fases planteadas en el procedimiento metodológico ya presentado anteriormente y destacando que la industria se encontró con condiciones de seguridad bastante incipientes y mucha informalidad.

La mayoría de las empresas, con información basada en el diagnóstico inicial de necesidades y estado de la seguridad de la información, resultaron, la gran mayoría sin políticas de seguridad informática, aun cuando se encontró un pequeño porcentaje de excepciones. Mayor información y detalles sobre los resultados del análisis y evaluación de riesgo cibernético sectorial se puede encontrar en (Acevedoarango y Echeverri L, 2025a) [1]

La revisión de estándares y selección de controles, aunado a la necesidad de aterrizar el prototipo cibernético protectivo, permitiendo la adecuada visibilización y asimilación del modelo, originó el nuevo marco CCCI. Dicho prototipo de ciberseguridad se muestra, a continuación, en la Figura 9, a saber:

Figura 9. Modelo de ciberseguridad para la industria flexográfica basado en el nuevo marco del Cubo de Campanito de Ciberseguridad Industrial (CCCI). **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. Autoría propia.



Nota. Modelo de ciberseguridad para la industria flexográfica basado en el nuevo marco del Cubo de Campanito de Ciberseguridad Industrial (CCCI) (compuesto por todos los cubos de la imagen, incluida la contribución de McCumber). **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1]. Autoría propia.

Para mayor detalle y comprensión de todos los pasos del modelo de ciberseguridad desarrollado para la industria flexográfica y que fue obtenido con la aplicación del nuevo marco CCCI, se tienen:

Paso 1. Evaluar el nivel de riesgo conociendo el estado y necesidades de la seguridad de la información de la empresa

La evaluación de riesgos es la base de la protección efectiva que brinda el modelo de ciberseguridad, ya que permite identificar vulnerabilidades en la infraestructura digital. Al efecto, se debe aplicar una metodología formal (ISO/IEC 27005, OCTAVE, o NIST, etc.) para calcular probabilidad e impacto de los eventuales ciberincidentes, categorizando activos críticos de la infraestructura informática. El resultado del análisis y evaluación del riesgo permite priorizar los recursos en áreas de mayor exposición.

- Realizar un autodiagnóstico preliminar basado en ISO 27001 y/o NIST 2.0 CSF, o ambos.
- Evaluar el nivel de riesgo informático utilizando una matriz de riesgos alineada con los procesos críticos de la empresa.

Paso 2. Definir e implementar una Política Corporativa de Seguridad de la Información

Una política de seguridad informática es otra base fundamental del modelo de ciberseguridad y se

recomienda que, aparte de ser adaptada a las necesidades y requerimientos de la empresa, este alineada con la norma ISO 27001, estableciendo las directrices estratégicas y las obligaciones mínimas que se deben considerar para proteger la información sensible.

- Elaborar una Política Corporativa de Seguridad Informática acorde a las particularidades de la empresa.
- Difundir y aplicar la Política Corporativa de Seguridad Informática, asegurando su comprensión en todos los niveles.

Paso 3. Seleccionar y adaptar un marco de trabajo con base en referentes internacionales de seguridad informática

Adoptar referentes internacionales ampliamente aceptados, combinando o eligiendo entre la familia normativa ISO 27000 series, el marco como NIST CSF 2.0 CSF o los CIS Controls, permitirá lograr la estandarización de los procesos de protección digital. Para las PYMEs de la industria flexográfica, lo más recomendable desde la perspectiva de la efectividad y la practicidad es realizar una combinación optando por una mezcla híbrida de los controles seleccionados, ajustando la complejidad técnica y práctica, así como considerando los costos necesarios.

De otra parte, usar la estructura de gobernanza del marco NIST CSF 2.0 CSF, la priorización de riesgos de la normatividad ISO 27000 series y la aplicabilidad técnica de los CIS Controls es lo más recomendable, tanto técnica como económicamente, pues esto asegura una protección integral sin sobrecargar los escasos y limitados recursos de las PYMEs y facilitando su adopción para mejores resultados.

- Elegir el marco de referencia (ISO 27001, NIST 2.0 CSF, CIS Controls, u otro reconocido).
- Adaptar el marco a la estructura, tamaño y recursos disponibles en la empresa.

Paso 4. Seleccionar un conjunto de controles apropiados para mitigar y reducir el riesgo

La selección de controles es otra etapa clave de la protección cibernética, la cual, acorde con las particularidades de cada empresa, debe efectuarse considerando la priorización y la proporcionalidad al nivel de riesgo al elegir cada uno de los controles.

De igual manera, la criticidad de los activos informáticos debe ser considerada para que la selección de los controles sea idónea, efectiva y eficaz. Complementariamente, los controles seleccionados deben mapearse contra los estándares elegidos para garantizar la consistencia y contar con capacidad de auditoría futura.

- Identificar controles alineados a los riesgos críticos detectados.
- Priorizar la implementación según impacto en la continuidad del negocio y en factibilidad práctica de su aplicación.

Paso 5. Establecer un programa de concientización y capacitación en ciberseguridad continuado y permanente

El factor humano es el eslabón más débil y uno de los mayores vectores de ciberataque, razón por la que un programa de capacitación y formación continua ayuda a mitigar los riesgos, mejorar la ciberdefensa y fortalecer la posición de seguridad informática. En particular, en el caso de la industria flexográfica este paso es crucial y obligatorio y quizá el que, en el corto plazo y con inmediatez, brinde mejores resultados.

Entrenar, tanto a personal administrativo, comercial, de mercadeo, de logística, de servicios generales, como, también, a personal operativo y de planta que, interactúa, o no, con sistemas informáticos, garantizará atender esta falencia y mitigar el riesgo, pues este paso garantiza que todos en la organización reconozcan ciberamenazas y apliquen protocolos básicos de seguridad.

- Diseñar programas de formación continua.
- Incluir simulacros de phishing, buenas prácticas de manejo de información y uso seguro de dispositivos.
- Utilizar el CCCI como herramienta pedagógica y didáctica de capacitación.

Paso 6. Fortalecer la seguridad tecnológica y de la infraestructura

La protección tecnológica requiere de la aplicación de técnicas y procedimientos de hardening para la infraestructura informática, incluyendo hardware, software, aplicativos, redes y bases de datos.

De otra parte, incorporar los principios de *Zero Trust Architecture* permitirá mejorar automáticamente el nivel de protección de las infraestructuras y activos críticos.

- Implementar medidas técnicas: firewalls, segmentación de red, cifrado, backups, autenticación multifactor (MFA), etc.
- Asegurar la actualización periódica de sistemas y aplicaciones (*Parcheo*).
- Disponer cualquier otra medida de seguridad técnica que se considere necesaria.

Paso 7. Implementar un sistema de monitoreo y detección de incidentes

El monitoreo continuo de la infraestructura y activos informáticos críticos, adoptando un SIEM como Azure

Sentinel, de pago, o, Wazuh, gratuito por ser *open source*, permitirá a las PYMEs y empresas, correlacionar eventos cibernéticos y detectar anomalías en tiempo real.

En la industria flexográfica, este aspecto es elemento clave en la constante vigilancia del tráfico de red, así como, también, los accesos no autorizados, los intentos de intrusión, entre otros vectores maliciosos, pues, esto reduce significativamente la ventana de exposición ante ciberataques.

- Desplegar herramientas de monitoreo (SIEM, IDS/IPS, EDR) siendo posible optar por alternativas de pago u *open source* según la capacidad particular de la compañía.
- Establecer métricas de detección temprana y alertas sobre anomalías en la red y sistemas.

Paso 8. Establecer un protocolo de respuesta a incidentes de ciberseguridad

Un plan de respuesta formal que defina roles, responsabilidades y flujos de comunicación ante ciberincidentes, que incluya procedimientos de contención, aislamiento, análisis forense digital, erradicación y recuperación, contribuye sustancialmente a mitigar el riesgo informático.

En un entorno productivo, la rapidez de respuesta es esencial para evitar la detención de la cadena de producción, en particular, de las líneas de impresión flexográfica, redundando en mayor capacidad de continuidad y resiliencia operacional.

- Diseñar un plan de manejo de incidentes de seguridad, con roles y responsabilidades claramente definidos y asignados.
- Formar un CSIRT interno (o *externo*) para la gestión y documentación de incidentes cibernéticos extrayendo las lecciones aprendidas.

Paso 9. Implementar un plan de continuidad del negocio (BCP)

El BCP ayuda a robustecer la operatividad mínima de los procesos críticos aún bajo ciberataque o fallo tecnológico, en razón a que contempla alternativas procedimentales claras y predefinidas para mantener, o restablecer con inmediatez, la operación de la cadena de producción, aunque los sistemas informáticos estén comprometidos.

En la industria flexográfica esto puede significar la priorización manual de órdenes y mantener sistemas de respaldo para fortalecer la continuidad y la resiliencia operacionales, practicando la premisa estratégica de prepararse para lo peor, mientras se espera lo mejor.

- Adaptar e implementar un plan de Continuidad (BCP), de tal manera que queden definidas las

estrategias de pronto restablecimiento digital y las actividades mínimas necesarias para mantener las operaciones críticas.

- Realizar pruebas periódicas de continuidad.

Paso 10. Implementar un plan de recuperación ante desastres (DRP)

El DRP establece procedimientos para restaurar la infraestructura tecnológica tras un ciberincidentes mayor (malware, ransomware, fallos de servidores, calamidades o desastres, etc.), razón por la que incluye alternativas de protección como copias de seguridad, redundancia en la nube, planes de restauración de sistemas y de software, con tiempos de recuperación (RTO/RPO) definidos según criticidad.

- Adaptar e implementar un plan de Recuperación de Desastres (DRP), de tal manera que queden definidas las estrategias de resiliencia digital mínimas necesarias para resistir eventos imprevistos y súbitos manteniendo las operaciones críticas.
- Realizar pruebas periódicas de recuperación.

Paso 11. Realizar auditorías, revisiones y pruebas de seguridad periódicas

Las auditorías de seguridad informática permiten verificar el cumplimiento de los controles y detectar las brechas de ciberseguridad.

Se recomienda combinar revisiones de cumplimiento acordes con la norma ISO 27001 con pruebas de naturaleza técnica, como procedimientos de pentesting, escaneo de vulnerabilidades, et al.

Para la industria flexográfica, estas revisiones y evaluaciones deben cubrir tanto los entornos informáticos de la cadena de producción interconectados al ciberespacio o a otras redes, como también, las demás redes de la empresa.

- Efectuar auditorías internas (y, eventualmente, auditorías externas).
- Realizar pruebas de penetración (*pentesting*), vulnerabilidad y análisis forense preventivo acorde con la capacidad de la compañía.

Paso 12. Establecer un ciclo de mejora continua en ciberseguridad

El ciclo Deming o ciclo PHVA es otra de las bases fundamentales del modelo de Ciberseguridad propuesta, pues, este ciclo asegura que el sistema de seguridad informática evolucione frente a nuevas amenazas, mejorando continuamente todos sus elementos y componentes, aprovechando el poder de la retroalimentación. Involucra actualizar políticas, ajustar controles, reevaluar riesgos y sacar e implementar las conclusiones de las lecciones aprendidas tras auditorías

y análisis forenses digitales de ciberincidentes, pues esto permite que la empresa mantenga y fortalezca su capacidad de continuidad y resiliencia digital en el tiempo.

- Aplicar el ciclo Deming (*Ciclo PHVA: Planear, Hacer, Verificar y Actuar*) como parte de la estrategia de ciberseguridad corporativa.
- Retroalimentar el modelo con lecciones aprendidas de incidentes, auditorías y cambios regulatorios, de negocios, de tecnologías, etc.
- Estructurar la documentación de los procedimientos de seguridad informática.
- Definir indicadores de gestión para medir la eficacia del modelo de ciberseguridad implementado.

Con el fin de lograr la consolidación del modelo de ciberseguridad propuesto para la industria flexográfica, con base en los aspectos ya mencionados, como la revisión de los estándares internacionales de mayor aceptación, las buenas prácticas de seguridad informática, los resultados derivados del diagnóstico sectorial del estado y requerimientos de la seguridad de la información (*consolidados en la respectiva matriz de riesgos y mapa de calor*), y de igual manera, en otros aspectos relevantes de carácter técnico, se desarrolló el prototipo anteriormente presentado en la Figura 9.

Para ello, y considerando, también, que se requiere de un modelo de ciberseguridad técnicamente robusto, pero, fácilmente entendible y comprensible para personal no especializado, en particular, gerentes, directores y personal operativo sin mayor conocimiento en ciberseguridad, se optó por adoptar, como base pedagógica y técnica, para la visualización y asimilación del prototipo de ciberseguridad de la industria flexográfica, el nuevo marco CCCI.

Al efecto, el CCCI extiende las dimensiones originales del constructo conceptual original de (*McCumber, 1991*) [2], incluyendo: los objetivos de seguridad informática, los mecanismos o contramedidas de seguridad informática y estado de los datos y, adicionando y extendiendo las dimensiones de estándares referentes internacionales, la implementación operativa y, la no menos importante, dimensión de la continuidad operativa y la resiliencia industrial y constituye un marco robusto y actualizado para la protección cibernética.

Otros resultados parciales de interés

A continuación, se presentan otros resultados parcialmente obtenidos, pues, como ya se consignó, se trata de una investigación todavía en proceso, pero, que igualmente, ofrece consideraciones interesantes y la posibilidad de trabajos de investigación futuros, a saber:

La ampliación, complementación, mejoramiento y actualización del marco de McCumber, consolidado a

través de la creación del marco CCCI, potencia sus características originales y aporta aún mayores ventajas para la ciberdefensa en profundidad que, actualmente, se requiere en sectores industriales esenciales; lo que se suma a que, también, como resultado adicional, favorece la comprensión y fácil asimilación de los modelos de ciberseguridad, por parte de personal no especializado, incluidos gerentes, mandos medios y personal operativo de planta, ya que, a través de elementos didácticos sencillos, se puede mejorar la cognoscibilidad y el aprendizaje significativo del modelo de ciberseguridad específico en cada organización, al vincular conceptos técnicos con situaciones reales de gestión de la información derivadas del marco CCCI.

Así, desde una perspectiva puramente pedagógica y didáctica, el modelo de ciberseguridad soportado en el nuevo marco CCCI, fomenta una comprensión progresiva y estructurada, transformándola en conocimiento organizacional, donde cada eje dimensional puede abordarse individualmente, lo que permite modular y adaptar su enseñanza a diferentes niveles de formación (básico, intermedio o avanzado).

Por ejemplo, en los niveles introductorios, se puede comenzar únicamente con la explicación de las seis dimensiones básicas, es decir, los principios y objetivos de la seguridad de la información, los estados de la información y las estrategias y mecanismos de seguridad informática, y avanzar, gradualmente, con la incorporación de las diversas convergencias de sus respectivas categorías, tanto bidimensionalmente al principio, como, tridimensionalmente después, hasta alcanzar una comprensión holística de todas las capacidades que ofrece el nuevo marco CCCI.

En este sentido, el valor del CCCI como herramienta didáctica, también, reside en su capacidad para traducir conceptos técnicos complejos a un lenguaje sencillo y de manera visual e intuitiva, haciéndolo accesible a públicos no especializados, como gerentes, ejecutivos, líderes de proceso, personal administrativo e incluso, a operadores y personal de planta.

Lo anterior, sin descuidar su eficiencia, eficacia y amplia capacidad de ciber-protección, la cual convierte al nuevo marco CCCI en un recurso pedagógico y didáctico ideal para la alfabetización digital en ciberseguridad, la formación continua en empresas y, adicionalmente, la formación en sectores industriales similares con una alta dependencia tecnológica y un proceso productivo altamente expuesto a las ciberamenazas, como es el caso de la industria flexográfica.

Así pues, el nuevo marco CCCI puede ser utilizado y servir como una base sólida para representar los componentes de un sistema de ciberdefensa alineado con los estándares internacionales, destacando su calidad como una excelente estrategia técnica y

pedagógica para el desarrollo de contenido protectivo y, también, educativo, académico y de investigación, como es el caso de la tesis de maestría en seguridad informática, objeto de este trabajo de investigación.

Además, desde una perspectiva de ciberdefensa en profundidad, tanto el constructo ideado por McCumber como el nuevo marco CCCI, pueden combinarse con otras normas internacionales como ISO 27001 (ISO/IEC, 2022) [8], el NIST 2.0 CSF (NIST, 2024) [7], o los CIS Controles (Dávila y Muñoz, 2023) [9], lo que refuerza su aplicabilidad práctica y relevancia cibernética de protección, y también, su dimensión educativa como herramienta de aprendizaje. Esta complementariedad fortalece su uso en contextos académicos para la formación técnica, permitiendo a aprendices, principiantes, novatos y personas sin formación especializada comprender y asimilar fácilmente no solo los principios conceptuales, sino también su implementación en entornos industriales reales, como el sector flexográfico.

El nuevo marco CCCI, como recurso didáctico y herramienta estratégica, pedagógica y técnica, se consolida y legitima ingenieril, investigacional, innovativa, pedagógica y educativamente, al vincularlo con marcos teóricos reconocidos, que respaldan su aplicabilidad en entornos de la industria real, pero, también, en escenarios educativos y académicos, tanto técnicos, como profesionales y de postgrado. Al respecto, se puede observar un resumen bastante conciso en (Acevedorango y Echeverri L., 2025b) [26].

Al respecto y como ejemplo, desde una perspectiva constructivista, el CCCI promueve la construcción activa del conocimiento al permitir a los gerentes y las altas directivas, al personal administrativo, a personal de planta, personal técnico y de ciberseguridad, investigadores, docentes, estudiantes, o a quien interese, modelar escenarios reales de ciberseguridad industrial, integrando variables técnicas, organizacionales y humanas en un entorno de análisis contextualizado.

Esta interacción estimula el pensamiento crítico y la resolución de problemas, pilares del aprendizaje significativo. Además, y en consonancia con el enfoque de aprendizaje significativo propuesto por Ausubel, el CCCI facilita la conexión entre nuevos conceptos y conocimientos previos al presentar situaciones que requieren interpretación, toma de decisiones y reflexión estratégica.

Se debe destacar, también, que la estructura modular del CCCI permite el diseño de experiencias de aprendizaje alineadas con los principios de diseño instruccional, adaptables a diferentes niveles de formación, objetivos pedagógicos y perfiles de usuario. Esto lo convierte en una herramienta versátil para la

planificación de secuencias didácticas orientadas al desarrollo de competencias en ciberseguridad.

Desde una perspectiva conectivista, el CCCI se proyecta como un centro de conocimiento que articula conocimientos técnicos, pedagógicos y organizacionales, promoviendo el aprendizaje colaborativo y el desarrollo continuo en entornos digitales.

Esta convergencia teórica legitima al CCCI como un objeto de aprendizaje robusto y escalable, alineado con los principios de los recursos educativos abiertos (REA) y los objetos de aprendizaje (OA), con potencial suficiente para integrarse en propuestas formativas innovadoras.

Por otro lado, al traducir conceptos técnicos complejos en estructuras visuales accesibles, aterrizadas y didácticamente asimilables, el marco CCCI se presenta de forma inherente y natural, como una herramienta pedagógica innovadora para la enseñanza de la ciberseguridad industrial en organizaciones y otros entornos. Su diseño tridimensional permite la representación clara de las capas de protección, los componentes críticos y los vectores de riesgo en las infraestructuras industriales, trascendiendo la mera impresión flexográfica de la que se originó, facilitando la comprensión y el entendimiento por parte de personas no especializadas en el campo de la seguridad informática.

Esta capacidad para superar la abstracción y visualizar con claridad la ciberseguridad conecta directamente al CCCI con teorías del aprendizaje como el constructivismo, el aprendizaje significativo y el diseño instruccional, que promueven la construcción activa del conocimiento, la conexión con experiencias previas y la aplicación contextualizada del conocimiento técnico. Así pues, desde una perspectiva metodológica, el CCCI permite la implementación de estrategias activas que fortalecen el proceso de enseñanza-aprendizaje.

Puede utilizarse en casos prácticos para analizar incidentes cibernéticos reales, así como en proyectos colaborativos donde los estudiantes diseñan soluciones aplicadas, o en dinámicas gamificadas que fomentan la exploración y la toma de decisiones. Además, su modularidad facilita la segmentación temática, permitiendo itinerarios de aprendizaje flexibles adaptados a diferentes niveles de formación según sea necesario.

En contextos híbridos o virtuales, su interoperabilidad lo hace compatible con diversas plataformas educativas, ya que puede adaptarse a las necesidades informáticas de las plataformas de e-learning, ampliando su alcance y relevancia en programas de educación superior, formación corporativa y simulaciones técnicas.

En resumen, el marco CCCI ilustra cómo una herramienta técnica puede reconceptualizarse como una solución educativa eficaz, contribuyendo a cerrar brechas de conocimiento y fortaleciendo la ciber-resiliencia en sectores industriales clave de la economía real, en beneficio de la sociedad y del país.

V. Discusión

Reflexiones sobre la utilidad y aplicación del CCCI como herramienta pedagógica y técnica.

A continuación, se discuten algunos aspectos interesantes sobre los aportes y contribuciones técnicas y pedagógicas del nuevo marco CCCI:

El marco CCCI innova, sobre la idea original de McCumber, al ofrecer un enfoque más actualizado, accesible, modular, extendido, complementado y pedagógicamente sólido para la ciberseguridad, pues al igual que su antecesor, está en capacidad de realizar funciones de seguridad informática similares, pero, contextualizadas a las industrias esenciales actuales.

En efecto, el CCCI permite simplificar conceptos técnicos complejos mediante una estructura didáctica visual e intuitiva, lo que facilita su comprensión, asimilación, aplicación y uso por parte de personas no especializadas, como gerentes, operadores y personal administrativo.

EL diseño logrado para el CCCI favorece el aprendizaje progresivo, permitiendo a los educadores adaptar la instrucción en niveles básico, intermedio y avanzado. Al vincular las dimensiones técnicas con escenarios reales de gestión de la información, CCCI promueve un aprendizaje significativo y fortalece el conocimiento organizacional.

De otra parte, al estar basado en teorías educativas como el constructivismo, el aprendizaje significativo y el conectivismo, el nuevo marco CCCI fomenta la construcción activa del conocimiento, el pensamiento crítico y el análisis contextual. Su modularidad permite estrategias didácticas flexibles, incluyendo estudios de caso, proyectos colaborativos y aprendizaje gamificado.

El marco, como tal, se integra y se alinea con estándares internacionales, como la norma ISO 27001, el marco NIST 2.0 CSF y los CIS Controls, mientras que, también, es adaptable a plataformas híbridas y digitales, lo que lo hace idóneo para sectores industriales con alta dependencia tecnológica, como la industria flexográfica, así como, también, para entornos académicos y de formación corporativa.

En última instancia, CCCI funciona tanto como marco orientador para el diseño de modelos de ciberseguridad, y como herramienta estratégica de enseñanza para construir resiliencia y fomentar la toma de decisiones

informadas en organizaciones de sectores industriales esenciales.

La integración entre BPM y un modelo dimensional aplicando minería de procesos permitió obtener una solución dinámica y flexible para la gestión de procesos de negocio, que mejora la eficiencia en las etapas de modelado, automatización, integración, monitoreo y optimización en forma frecuente.

VI. Aclaraciones y trabajos futuros.

Como ya se ha mencionado anteriormente, si bien esta investigación enfatiza el potencial pedagógico del nuevo marco CCCI como herramienta para visualizar y aplicar conceptos de ciberseguridad industrial, también, reconoce limitaciones clave en su implementación actual, en razón a que la innovación realizada, proviene de una tesis de maestría aún en desarrollo y esto ocasiona que, aún y a fecha presente, su estrategia pedagógica carezca todavía de descripciones detalladas de las metodologías, recursos y entornos de aprendizaje necesarios para su apropiación efectiva por parte de empresas y audiencias no especializadas.

Al respecto, y en aras de validar la efectividad del CCCI, tanto técnica como pedagógicamente, los trabajos de investigación futuros deben incluir estrategias de verificación empíricas como estudios de caso, programas piloto y encuestas de percepción que involucren tanto a personal conocedor en seguridad informática, como, también, a persona no experto, en entornos empresariales donde se pueda implementar el nuevo marco CCCI.

Estos esfuerzos ayudarán a medir su impacto en el aprendizaje, la adaptación y la toma de decisiones en entornos industriales, particularmente en PYMEs, así como, también su eficacia y efectividad pedagógica y técnica. Abordar las brechas procedimentales y metodológicas del marco CCCI, en su calidad de una innovación heredera de las bondades y ventajas del cubo de McCumber, fortalecerá su legitimidad técnica y pedagógica, permitiendo la consolidación de métricas y de evidencia para una aplicación más amplia en la industria real. En última instancia, esto posicionará al CCCI no sólo como un recurso didáctico, sino, también, como un marco de ciberseguridad robusto y capaz de proteger infraestructuras de producción críticas proporcionando una ciberdefensa efectiva en profundidad para pymes y empresas.

VII. Conclusiones

Aunque el “Cubo de McCumber de la Seguridad Informática” sigue siendo un modelo técnico, pedagógico y educativo valioso, sus limitaciones para abordar las necesidades actuales de ciberseguridad

especialmente en sectores industriales con infraestructura crítica de producción, hicieron necesaria su expansión conceptual mediante un proceso ingenieril de innovación basado en el mejoramiento de su constructo conceptual original.

El nuevo marco CCCI introduce tres nuevas dimensiones, expandiendo, reconfigurando y actualizando el constructo original del “Cubo de McCumber de la Seguridad Informática” en un recurso técnico y pedagógico que, respalda tanto la modelación técnica como la implementación educativa. Esta doble función le permite servir como marco de referencia alineado con estándares internacionales (*Normas ISO 27000 series, NIST 2.0 CSF, y CIS Controls*), así como herramienta de formación para la alfabetización digital, la continuidad operativa y la resiliencia organizacional.

Diseñado con modularidad e interoperabilidad, el nuevo marco CCCI puede adaptarse a diversos entornos de industriales, técnicos, pedagógicos y de aprendizaje, siendo adaptable y personalizable ante diversos y variados perfiles de audiencia y/o de necesidades dinámicas y variables a nivel técnico, pues, su estructura permite rutas metodológicas, técnicas y didácticas flexibles y segmentación temática, lo que lo hace idóneo para entornos industriales, entrenamiento en organizaciones, e incluso para uso en programas académicos, capacitaciones corporativas y simulaciones empresariales.

Al representar visualmente los riesgos, ciberamenazas y capacidades de defensa, el nuevo marco CCCI contribuye a la formación de personal ciberresiliente en todos los sectores (*industriales, organizacionales, técnicos, académicos, de investigación, etc.*) y no solo en la flexografía, sino, también, en cualquier industria donde la seguridad digital sea un punto esencial por atender. De esta forma, el nuevo marco CCCI se basa en principios clave de diseño en seguridad informática, pero, también, tiene aplicación directa en el ámbito educativo, lo cual potencia su efectividad como recurso especializado de formación.

En este sentido, el nuevo marco CCCI está orientado a alcanzar objetivos técnicos y pedagógicos específicos, como la comprensión de los riesgos, las diversas amenazas y vulnerabilidades cibernéticas, y las distintas capas de defensa en profundidad como procesos críticos de protección en infraestructuras industriales esenciales. Esto contribuye al desarrollo de personal más consciente, mejor capacitado y estratégicamente ciber-resiliente, no solo en flexografía, sino en todos los sectores e industrias.

La estructura tridimensional del CCCI permite una alta reutilización, ya que puede adaptarse a distintos niveles de profundidad y a audiencias técnicas o no técnicas. La flexibilidad y modularidad del modelo facilita su

descomposición en componentes temáticos independientes, permitiendo la construcción de rutas de aprendizaje flexibles y personalizadas. Además, su interoperabilidad garantiza compatibilidad con diversas herramientas tecnológicas, plataformas digitales y entornos de capacitación y enseñanza, facilitando su integración en el entorno industrial, pero, también, en programas académicos, capacitaciones corporativas o simulaciones industriales.

De otra parte, a la fecha, la investigación avanzada se encuentra a un 98% y está *ad portas* de ser finalizada. Sus resultados parciales revelaron que, en la industria flexográfica, y aunado a los recursos financieros, la principal barrera para la adopción de modelos de ciberseguridad no era su diseño técnico, sino, más bien, la dificultad para entenderlos, asimilarlos, e implementarlos, especialmente entre tomadores de decisiones, como gerentes y altas directivas, y entre personal sin formación especializada en ciberseguridad.

En este contexto, el factor humano sigue siendo una vulnerabilidad central en la defensa cibernética, y el nuevo marco CCCI lo aborda promoviendo la conciencia, la comprensión y el pensamiento estratégico. Su orientación pedagógica permite desarrollar contenidos educativos que favorecen el aprendizaje significativo, el análisis crítico y la integración de la ciberseguridad en la cultura organizacional, sin perder de vista la necesidad de una defensa cibernética efectiva.

La industria flexográfica, recientemente reconocida como crítica debido a las interrupciones causadas por la pandemia de COVID-19, enfrenta crecientes amenazas cibernéticas que exigen soluciones de ciberseguridad robustas y escalables. Sus PYMEs, en particular, requieren modelos de protección cibernética que fortalezcan las estrategias de defensa en profundidad y mejoren las capacidades de protección de la confidencialidad, integridad y disponibilidad de la seguridad de la información de la infraestructura informática asociada a la gestión, operación y control de su cadena de producción crítica, puesto que la creciente sofisticación y frecuencia de los ciberataques han convertido a este sector, como a muchos otros, en un objetivo para actores maliciosos, lo que resalta la urgencia de implementar marcos de ciberseguridad efectivos, adaptados a sus vulnerabilidades tecnológicas y operativas y que sean entendibles para las empresas.

De otro lado, es importante anotar que, durante el proceso de investigación realizado, surgieron desafíos imprevistos, especialmente la necesidad de hacer que los modelos de ciberseguridad fueran comprensibles, visualizables y aplicables para gerentes y personal no especializado, lo cual condujo al desarrollo del nuevo marco CCCI como un resultado colateral de alto valor

agregado, particularmente, incluyendo un significativo componente de innovación.

Las necesidades que llevaron a la creación del CCCI no fueron únicamente de naturaleza técnica, sino, también, de índole pedagógica y educacional, lo que motivó la búsqueda de una herramienta didáctica capaz de cerrar la brecha entre conceptos complejos de ciberseguridad y su adopción organizacional. El nuevo marco CCCI, como una versión evolucionada, complementada, mejorada, actualizada y ampliada del “Cubo de McCumber de la Seguridad Informática”, responde a este reto, ofreciendo una estructura modular de alto valor agregado, no solo técnico, sino, también, pedagógico, que facilita la visualización, comprensión y adopción entre gerentes y personal operativo.

VIII. Agradecimientos, Autores y afiliaciones

Agradecimientos

Los autores expresan su agradecimiento a:

Serviflex Arco Internacional S.A.S. y Serviflex Arco USA LLC (empresas patrocinadoras); a la industria flexográfica colombiana; al Instituto Tecnológico Metropolitano (I.T.M.) de Medellín; al Politécnico Colombiano Jaime Isaza Cadavid de Medellín (P.C.J.I.C.); al Instituto Tecnológico de Antioquia, Medellín (T.de.A.); a la Agencia de Educación Superior de Antioquia (Sapiencia); a la Universidad Nacional de Colombia, Seccional Medellín, Facultad Nacional de Minas (UNALMED); a la Universidad de Antioquia (U.de.A.); a la Universidad EAFIT; a la Universidad de Medellín (U.de.M.); al MinTIC; al Centro de Desarrollo Integrado (CENDI);

A todos nuestros profesores: Ing. Héctor Fernando Vargas Montoya; Ing. Francisco Eugenio López Giraldo, *Ph.D.*; Ing. Juliver de Jesús Gil Herrera, *Ph.D.*; Ing. Leonel Marín Ramírez; Ing. Sergio A. Álvarez G.; Ing. Juan F. Puerta Grajales; Ing. Andrés Alberto Gómez Acosta; Ing. Alex Mauricio Ávila Quiceno; Ing. Héctor Valencia Valencia; Ing. Fredy Humberto Gómez Orjuela; Ing. Hernán Francisco Villar Vega; Ing. Julián Andrés Naranjo Londoño; Ing. Jorge Ernesto Espinosa Oviedo, *Ph.D.*; Ing. Sixto Enrique Campaña Bastidas, *Ph.D.*; Ing. Darío Enrique Soto Durán, *Ph.D.*; Ing. Juan Camilo Giraldo Mejía, *Ph.D.*; Ing. Juan Carlos Rodríguez Gamboa, *Ph.D.*; Ing. Santiago Arboleda Quiroz; Ing. Fredy Alonso Vidal Alegría (Unimayor-Cauca).

También, a las directivas de I.T.M. , en particular, al honorable Abogado Don Alejandro Villa Gómez (*Rector, I.T.M.*); al Ing. Eduard Alberto García Galeano (*Virrektor Financiero, I.T.M.*); a la Ing. Elizabeth Rodríguez Acevedo (*Decana, Facultad de Ingeniería, I.T.M.*); a la Ing. Olga Lucía Henao Pardo (*Decana, Facultad de Ingeniería, P.C.J.I.C.*); a la Ing. Adriana Xiomara Reyes Gamboa, *Ph.D.* (*Directora del Programa de Doctorado*

de I.T.T., P.C.J.I.C.); Ing. Gladis Helena Vásquez Echavarría (*Directora de la Especialización en Analítica de Datos, P.C.J.I.C.*); a la Ing. Aixa Eileen Villamizar Jaimes (*Coordinadora de la Maestría en Gestión de Tecnología de la Información y de la Especialización en Seguridad de la Información, T.de.A.*)

A nuestros compañeros: Ing. Francisco Antonio Gutiérrez Calderón (I.T.M./Masglobal Consulting); Ing. Orlando Villabona Bolaños (I.T.M.).

Además, los autores agradecen a las compañías tecnológicas y corporaciones multinacionales, como CISCO; IBM; Alphabet Corp. (*Google, Gemini, YouTube*); Microsoft Corp.; OpenAI; AWS; y a todos los diversos YouTubers de ciberseguridad y áreas del saber afines, por brindar el acceso a sus recursos de E-Learning, conocimiento valioso y herramientas tecnológicas utilizadas en el desarrollo de los programas de posgrado de Especialización en Ciberseguridad y de Maestría en Seguridad Informática (I.T.M.) y Especialización en Analítica de Datos (P.C.J.I.C.), y que, sin duda alguna, ayudaron y participaron de nuestro camino de formativo en *Ethical Hacking*, en la elaboración de nuestra tesis de maestría en seguridad informática (M.S.I., I.T.M.) y en la consolidación de esta investigación innovadora (CCCI (ICTBC)), que dejamos como legado a nuestra industria flexográfica y convertidora y a la sociedad entera.

También, nuestro agradecimiento sincero, a todos aquellos que, por brevedad o humana e involuntaria omisión, no se mencionan expresamente, pero, que de alguna u otra manera colaboraron en este propósito.

Sobre los autores

Sobre los autores, su perfil, afiliaciones y contactos:

1 Ing. Edgar Alberto Acevedoarango.

Ingeniero Eléctrico (Universidad Nacional de Colombia, Facultad Nacional de Minas, Medellín); Magíster en Administración de Empresas – M.B.A. (Universidad EAFIT); Especialista en Negocios Internacionales (Universidad EAFIT); Especialista en Ciberseguridad (I.T.M.); Magíster en Seguridad Informática (c) (I.T.M.); Especialista en Analítica de Datos (c) (Politécnico Colombiano Jaime Isaza Cadavid).

Miembro 101531609 del Institute of Electrical and Electronics Engineers (IEEE); miembro 2202483 de la Information Systems Audit and Control Association (ISACA); miembro 27575645 del SANS Institute; miembro 2854043 del Open Worldwide Application Security Project (OWASP); miembro de la Rivest, Shamir & Adleman Conference (RSAC); miembro 27575645 de la Association for the Advancement of Artificial Intelligence (AAAI); miembro de la Association for Safe & Ethical Artificial Intelligence (IASEAI); miembro 429164 del International Council on Systems

Engineering (INCOSE) - Critical Infrastructure Protection, Artificial Intelligent Systems and Engineering for Industrial Systems communities del Capítulo Latinoamericano; miembro 2949019 del International Information Systems Security Certification Consortium ((ISC)2) (c); miembro 2343187 de la Internet Society (ISOC); miembro 1122027569 de The Institution of Engineering and Technology of United Kingdom (IET SSO, UK); miembro de la Asociación Internacional de Ciberseguridad (ASICI); miembro del Centro de Ciberseguridad Industrial (CCI); miembro de la Asociación Colombiana de Ingenieros (c) (ACIEM); miembro de la Sociedad Colombiana de Computación (SCO2); miembro de Asociación de Ingenieros Egresados de la Facultad Nacional de Minas (ADEMINAS), (UNALMED, Medellín.) y miembro de ResearchGate.

Gerente de Innovación, Proyectos, I+D y Nuevas Tecnología. Serviflex Arco USA LLC, Redondo Beach, CA, Estados Unidos de América y Serviflex Arco Internacional S.A.S. Medellín, Antioquia, Colombia.

ORCID: <https://orcid.org/0009-0001-1339-0517>.

Contacto: eea.researcher@gmail.com

Figura 10. Los creadores del marco CCCI (ICTBC) de protección cibernética de industrias esenciales y autores de este artículo. **Fuente:** Tomado de (Acevedoarango y Echeverri L, 2025a) [1].



Nota. Ing. Edgar Alberto Acevedoarango (Izquierda) e Ing. Adriana María Echeverri Londoño. (Derecha). **Fuente:** Tomado de Acevedoarango y Echeverri L, 2025a) [1].

2 Ing. Adriana María Echeverri Londoño.

Ingeniera Química (Universidad de Antioquia); Magister en Administración – M.B.A. (Universidad EAFIT); Especialista en Gerencia de la Calidad (Universidad EAFIT); Especialista en Ciberseguridad (I.T.M.); Magister en Seguridad Informática (c) (I.T.M.); miembro 101531882 del Institute of Electrical and Electronics Engineers (IEEE); miembro 2202484 de la Information Systems Audit and Control Association (ISACA); miembro 30398330 del SANS Institute; miembro 2854045 de la Open Worldwide Application Security Project (OWASP); miembro de la Rivest, Shamir & Adleman Conference (RSAC); miembro

429167 del International Council on Systems Engineering (INCOSE) - Critical Infrastructure Protection and Recovery, Resilient Systems, and Systems Engineering Quality Management (SEQM) communities of LatAm Chapter -]; miembro 2949063 del International Information Systems Security Certification Consortium ((ISC)2) (c); miembro 2343188 de la Internet Society (ISOC); miembro 1122027570 de The Institution of Engineering and Technology of United Kingdom (IET SSO, UK); miembro de la Asociación Internacional de Ciberseguridad (ASICI); miembro del Centro de Ciberseguridad Industrial (CCI); miembro de la Asociación Colombiana de Ingenieros (c) (ACIEM); miembro de la Sociedad Colombiana de Computación (SCO2) y miembro de ResearchGate

Gerente Comercial, Técnica y de Seguridad Informática. Serviflex Arco USA LLC, Redondo Beach, CA, Estados Unidos de América y Serviflex Arco Internacional S.A.S. Medellín, Antioquia, Colombia.

ORCID: <https://orcid.org/0009-0002-4525-076X>.
Contacto: ameltampo1212@gmail.com

IX. Referencias y Bibliografía

- [1] E.A. **Acevedoarango**, A.M. **Echeverri L.**: Diseño de un modelo de ciberseguridad para la cadena de producción crítica de la industria flexográfica. Tesis de maestría en seguridad informática (en curso). ITM, Medellín, Colombia (2025).
- [2] J.R. **McCumber**: Information Systems Security: A Comprehensive Model. In: 14th National Computer Security Conference, pp. 328–337. NIST/NCSC, Washington D.C., USA (1991). <https://csrc.nist.gov/files/pubs/conference/1991/10/01/proceedings-14th-national-computer-security-confer/final/docs/1991-14th-ncsc-proceedings-vol-1.pdf>
- [3] G. **Brito** Acuña, V. **Díaz** Blanco: Mejora de los procesos de ciberseguridad aeronáutica mediante un marco de madurez. Rev. Cubana Ciencias Informáticas. 17 (Supl.), 230–250 (2023). [https://rcci.uci.cu/?journal=rcci&page=article&op=view&path\[\]=2855&path\[\]=1156](https://rcci.uci.cu/?journal=rcci&page=article&op=view&path[]=2855&path[]=1156)
- [4] E.M. **Mejía** Cortez: El mercado de la flexografía en América Latina. Revista de Coyuntura Económica, Instituto de Investigaciones Económicas, San Salvador (2024). <https://revistas.ues.edu.sv/index.php/coyunec/article/download/423/355>
- [5] E.A. **Acevedoarango**: Sistemas de Control Digital en Subestaciones Eléctricas de Alta y Extra Alta Tensión. Tesis de grado en ingeniería eléctrica. Universidad Nacional de Colombia, Sede Medellín, Facultad Nacional de Minas. Medellín. (1997).
- [6] F. **Castiblanco**, L.A. **Oviedo** Regueros: Análisis de riesgos informáticos y propuesta de controles para su mitigación utilizando las normas ISO/IEC 27001, 27002 y 27005. Tesis de grado. UNAD, Bogotá, Colombia (2017). <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2660/Trabajo%20de%20grado.pdf>
- [7] **NIST**: NIST Cybersecurity Framework 2.0. US Department of Commerce. CSWP-29, 1–32 (2024). <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
- [8] **ISO**: ISO/IEC 27001:2022. International Organization for Standardization (2022). <https://www.iso.org/es/home>
- [9] M.C. **Dávila** Fernández, J. **Muñoz** Huaman: Diseño de controles de ciberseguridad para reducir ciberataques en empresas distribuidoras de productos digitales basados en el control CIS V8. Tesis de pregrado, Universidad Peruana de Ciencias Aplicadas. Lima, Perú (2023). https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/670133/Davila_FM.pdf
- [10] E.A. **Acevedoarango**, A.M. **Echeverri L.**: El Libro gordo de Anilox. Primer libro gordo de Serviflex Arco. Ed. Serviflex Arco Internacional S.A.S., 2nd ed. ISBN 978-958-56544-0-2. Medellín (2017). www.serviflexarco.com
- [11] E.A. **Acevedoarango**: Aplicación de los fenómenos electromagnéticos en la industria convertidora. Rev. Mundo Eléctrico 65(V17), Ed. Orvisa. Bogotá, Colombia. (2009). <https://www.mundoelectrico.com/edicion-n-65-20-anos>
- [12] E.A. **Acevedoarango**, A.M. **Echeverri L.**: El libro gordo del tratamiento Corona. Segundo libro gordo de Serviflex Arco. Ed. Serviflex Arco Internacional S.A.S., 3rd ed. ISBN 978-958-56544-1-9. Medellín (2017). www.serviflexarco.com
- [13] **Figura 1. Envapack.com**: Planta de flexográfica con línea de producción de última generación (Bobst). (2024). Image taken from: <https://www.envapack.com/2019/05/establecimiento-grafico-impresores-continua-creciendo-en-el-mercado-de-embalaje-flexible-con-impresoras-flexo-de-tambor-central-y-maquinas-laminadoras-bobst/>

- [14] J. Quintana, F. Cornejo y A. Rigail Cedeño. "Análisis y Diseño de Empaques Flexibles para Alimentos". *Paper*. Revista Tecnológica ESPOL, Vol. 20, N. 1, 11-18, ISSN: 0257-1749. Guayaquil, Guayas, Ecuador. Agosto - Octubre, 2007.
<https://rte.espol.edu.ec/index.php/tecnologica/article/view/156/100>
- [15] **Figura 2.** John R. MacCumber. R.S.A. Conference 2016 (RSAC16). Panóptico referencial de expertos conferencistas invitados. www.rsaconference.com. 2016.
<https://www.rsaconference.com/experts/john-mccumber>
- [16] W. V. Maconachy, C. D. Schou, D. Ragsdale and D. Welch: A model for information assurance: An integrated approach. *Revista Proceedings of the 2001 IEEE: Workshop on Information Assurance and Security*. Ed. IEEE, US Military Academy, West Point, NY, U.S.A. pp. 306-310. (2001).
<https://grothoff.org/christian/teaching/2007/3704/w2c3.pdf>
- [17] F.E. López Giraldo: Seminario I de metodología de la investigación (curso postgrado). Material Formativo, Especialización en Ciberseguridad. ITM, Medellín, Colombia. (Febrero de 2024).
<https://campusvirtual.itm.edu.co/>
- [18] C.R. Hernández Sampieri, C. Fernández Collado, P. Baptista Lucio: Metodología de la investigación. McGraw-Hill, Naucalpan, México (1991).
<https://www.academia.edu/102204834/>
- [19] J. Casas Anguita, J.R. Repullo Labrador, J. Donado Campos: La encuesta como técnica de investigación. *Rev. Atención Primaria* 31(8), 527–538 (2003).
<https://core.ac.uk/download/pdf/82245762.pdf>
- [20] H.F. Vargas Montoya: Seminario IV de metodología de la investigación (curso postgrado). Material formativo, Maestría en Seguridad Informática. ITM, Medellín, Colombia. (Agosto de 2024).
<https://campusvirtual.itm.edu.co/>
- [21] S.A. Álvarez Gaviria: Ciberseguridad y Redes (curso formativo de extensión). Diplomado en Ciberseguridad y Redes. Material formativo. Universidad de Antioquia (Convenio SAPIENCIA), Medellín (2024).
<https://ingenia.udea.edu.co/>
- [22] L. Marín R.: Análisis y gestión de riesgos (curso postgrado). Material Formativo, Especialización en Ciberseguridad. ITM, Medellín, Colombia. (Marzo de 2024).
<https://campusvirtual.itm.edu.co/>
- [23] **ESPOL Revista Tecnológica:** Metodología para el análisis y evaluación de riesgos aplicada a la seguridad informática bajo la norma ISO/IEC 27001. *Rev. Tecnológica – ESPOL* 28(5), (2015).
<https://rte.espol.edu.ec/index.php/tecnologica/article/view/456>
- [24] **Figura 9.** Funcionamiento práctico del "Cubo de McCumber de la Seguridad Informática".y, también, del "Cubo Campanito de Ciberseguridad Industrial (CCCI)". **National Cybersecurity Training & Educational Center (NCyTE Center):** The McCumber Cube and CIA Triad; E-Mate 2.0 (Online animation), National Science Foundation (NSF). (2025).
<https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons/the-mccumber-cube-and-cia-triad>
- [25] **National Cybersecurity Training & Educational Center (NCyTE Center):** The McCumber Cube and CIA Triad; E-Mate 2.0 (Online animation), National Science Foundation (NSF). (2024).
<https://www.ncyte.net/academia/faculty/cybersecurity-curriculum/college-curriculum/interactive-lessons>
- [26] E.A. Acevedoarango, A.M. Echeverri L.: Del cubo mágico a la ciberseguridad industrial. *Revista Institucional La Tekné*, ed. 2025-1, No. 116. ISBN 2744-8886, Ed. Fondo Editorial I.T.M. Medellín (2025).
<https://catalogo.itm.edu.co/gpd-la-tekhne-n-116--68ee8fb056f25.html>

ICTBC: ENGINEERING INNOVATIVE PROCESS DERIVED OF THE DESIGN OF AN INDUSTRIAL CYBERSECURITY MODEL BY IMPROVING THE MCCUMBER CUBE

Edgar Alberto Acevedoarango¹ y Adriana María Echeverri Londoño²

¹ Electrical Engineer (National University of Colombia, National Faculty of Mines, Medellín); Magister's Degree in Business Administration – M.B.A. (EAFIT University); Specialist's degree in International Business (EAFIT University); Specialist's degree in Cybersecurity (U. I.T.M.); Magister's Degree candidate in Computing Security (c) (U. I.T.M.); Specialist's degree candidate in Data Analytics (c) (Jaime Isaza Cadavid Colombina Polytechnic University). Member 101531609 of the Institute of Electrical and Electronics Engineers (IEEE); member 2202483 of Information Systems Audit and Control Association (ISACA); member 27575645 of the SANS Institute; member 2854043 of Open Worldwide Application Security Project (OWASP); member of Rivest, Shamir & Adleman Conference (RSAC); member 27575645 of The Association for the Advancement of Artificial Intelligence (AAAI); member of International Association for Safe & Ethical Artificial Intelligence (IASAI); member 429164 of International Council on Systems Engineering (INCOSE) - Artificial Intelligence Systems, Critical Infrastructure Protection and Recovery and Systems Engineering for Industrial Systems communities of LatAm Chapter -; member 2949019 of International Information Systems Security Certification Consortium ((ISC)²) (c); member 1122027569 of the Institution of Engineering and Technology of United Kingdom (IET SSO, UK); member of Asociación Internacional de Ciberseguridad (ASICI); member of Centro de Ciberseguridad Industrial (CCI); member 2343187 of Internet Society (ISOC); member of Blockchain Council (BCC); member of Asociación Colombiana de Ingenieros (ACIEM) (c); member of Sociedad Colombiana de Computación (SCO²); member of Asociación de Ingenieros Egresados de la Facultad Nacional de Minas (ADEMINAS UNALMED); and member of ResearchGate. Manager of Innovation, Projects, R&D, and New Technologies (Serviflex Arco Internacional S.A.S.). Medellín, Antioquia, Colombia.
Contact: eaa.researcher@gmail.com – ORCID: <https://orcid.org/0009-0001-1339-0517>.

² Chemical Engineer (University of Antioquia); Magister's Degree in Business Administration – M.B.A. (EAFIT University); Specialist's Degree in Quality Management (EAFIT Univ.); Specialist's degree in Cybersecurity (U. I.T.M.); Magister's Degree candidate in Computing Security (c) (U. I.T.M.). Member 101531882 of the Institute of Electrical and Electronics Engineers (IEEE), member 2202484 of Information Systems Audit and Control Association (ISACA), member 30398330 of SANS Institute, member 2854045 of Open Worldwide Application Security Project (OWASP), member of Rivest, Shamir & Adleman Conference (RSAC), member 429167 of International Council on Systems Engineering (INCOSE) - Critical Infrastructure Protection and Recovery, Resilient Systems, and Systems Engineering Quality Management (SEQM) communities of LatAm Chapter -; member 2949063 of International Information Systems Security Certification Consortium ((ISC)²) (c); member of Cybersecurity International Association (ASICI); member of Centro de Ciberseguridad Industrial (CCI); member 2343188 of Internet Society (ISOC); member 1122027570 of the Institution of Engineering and Technology of United Kingdom (IET SSO, UK); member of Blockchain Council (BCC); member of Asociación Colombiana de Ingenieros (ACIEM) (c); and member of the Sociedad Colombiana de Computación (SCO²); and member of ResearchGate. Commercial, Technical & Computing Security Manager (Serviflex Arco Internacional S.A.S.). Medellín, Ant., Colombia.
Contact: ameltempo1212@gmail.com - ORCID: <https://orcid.org/0009-0002-4525-076X>.

Abstract

This paper shows a proposal of a methodological innovation derived of the design of a cybersecurity model created for the Colombian's flexographic industry. The new approach is based on an innovative engineering process, realized by the improvement, updating and extending the McCumber cube, to be used like reference framework to support the development, design and implementation of cybernetic protection's prototypes for essential industries and critical productive sectors. As part of a master's thesis in computer security in progress, this research is focused in the Industrial Cybersecurity Tinker Bell Cube, ICTBC (Cubo Campanito de Ciberseguridad Industrial, CCCI, in Spanish), a collateral and unexpected result of the consolidation's activities of a cybersecurity's model to the digital protection of computational infrastructure that operates the critical productive chain's, particularly, in SMEs. In this context, ICTBC offers a new conceptual strategy and a practical tool to transmit very complex and technical concepts of cybersecurity to C.E.O.s, managers and non-specialized personnel, facilitating the understanding, assimilation, adaptation and implementation of cybernetic protection models in all organization levels of all kinds of critical industries.

Keywords: Cybersecurity, critical infrastructure, flexography, industry, McCumber's cube, pedagogy, risk.

1. Introduction

The increasing of automation and digitalization, coupled with the adoption of technologies like digital control systems (DCS), internet of things (IoT) and, more recently, of the artificial intelligence (AI), have significantly heightened cyber risk in the industry. This intensifies the need for robust industrial cybersecurity models to counter increasingly sophisticated attacks that compromise confidentiality, integrity, and availability in critical IT and computing infrastructures. As a solution, the Industrial Cybersecurity Tinker Bell Cube, ICTBC, was created and introduced, like very useful framework, to support the design of cybersecurity models for critical industries and to contribute for their understanding, adaptation and implementation. This new cybersecurity framework extends the original idea of the McCumber's cube, incorporating new dimensions to address current and future cyber challenges in critical industrial environments. So, the ICTBC aims to provide in-depth cybersecurity protection and facilitate its understanding, personalization and adoption by C.E.O., managers, leaders and non-specialized personnel, creating and promoting cybersecurity culture within organizations

In this ideas' order and like a new tool, the ICTBC is based on the application of an engineering innovation process, which was realized during the development of a design of a cybersecurity model for computing infrastructure associated to the operation and control of the critical productive chain of the flexographic industry [1], and which was based on the improvement of the McCumber cube of computer security [2], through its conceptual extension, its complementation, contextualization to industrial environments and necessary updating, consolidating an additional result unexpected and an interesting added value derived of the execution of the methodological proposal of the master's thesis.

The ICTBC is a partial result of a research work in progress, framed in the development of a master's thesis in computer security [3], and focused, particularly, on the context of SMEs (PYMEs in spanish) [4], [5] of the Colombian flexographic industry, but also, the potential of the ICTBC is applicable to another similar sectors, because the flexographic industry has similar characteristic in the criticality of their production chain like other production processes that are essentials sectors for the real economy, too. Due to its critical role [6] in the production of packaging [7], containers, printed boxes and labels, all of which are essential inputs for the supply chains of another critical strategic sectors such as food, pharmaceuticals and basic goods, the flexographic industry is an appropriate and suitable case of study. Consequently, in this point, it's necessary to note that the ICTBC can be extended to all kinds of essential industries with critical production chains.

2. Background, problem statement and significance

In this context, and in the face of increasing automation, the incorporation of digital control systems (DCS) [8], the internet of things (IoT) and, more recently, the accelerated adoption of digitalization and artificial intelligence (AI) [9] in the industries and business, a condition from which the flexographic industry is not exempt, who, like another critical productive sectors, faces the great challenge of a constant and ever-growing level of cyber exposure, due to an increasingly wide, large, and very difficult to protect and ensure the attack surface.

This scenario, coupled with the complexity, sophistication, and exponential increase in the frequency and quantity of cyberattacks, has highlighted the urgent need to have an industrial cybersecurity model that adopts international standards and good security practices, with the aim of guaranteeing the confidentiality,

integrity, and availability of information in IT and computing infrastructures associated with the management, control, and operation of essential production chains, as well as strengthening cyber defense in depth with the intention of developing or improving operational continuity and digital resilience in essential industries and productive sectors.

In this sense, an approach to the design of a cybersecurity model was proposed as a solution that, through the extension of the McCumber Cube, would integrate the principles and dimensions originally conceived by Eng. John McCumber (information security objectives, information states, and computer security mechanisms) [10], [11] and [12], together with the new dimensions added (international standards and references for computer security in accordance with [13], [14] and [15]; operational implementation (adaptability and flexibility, interoperability and integrability, and scalability, A.I.S.); and continuity and resilience according to [16], [17] and [18]) in order to respond effectively, efficiently and effectively to the current demands of cybersecurity in critical industrial environments such as those raised in the contributions of [19], [20] and [21].

The result of this research effort led to the creation of the “Industrial Cybersecurity Tinker Bell Cube, ICTBC, which allows not only the protection, defense in depth, evaluation, monitoring and auditing of the information security of the IT infrastructure, but also the easy and better understanding of the cybersecurity model and its application, adoption and implementation by C.E.O.s, managers and non-qualified personnel in cybersecurity of industrial organizations as its propose in a similar written collaboration for [22]. On the other hand, in reason that in the context of the research job conducted, no master's or doctoral research papers or thesis woks were found with the clear characteristic to support a design of a cybersecurity model in an improvement or update of the McCumber cube of computer security, the innovation derived from this engineering process of improving constitutes an advance in the application of theoretical and methodological frameworks of cybersecurity's model design, not only in the flexographic sector [23] also, and in general, in all another similar industries with essential production's lines, contributing to the sustainability and protection of critical infrastructures [24] for the real economy, the country, and society.

3. A brief approach to flexographic industry and their critical productive infrastructure

As can be inferred from the research work of [1], the flexographic industry is a key sector of the real economy that is dedicated to the production of flexible and rigid packaging, boxes, labels, containers and other products (see figure 1). All of them are essential parts of the supply chains of other equally critical industries, such as food, pharmaceutical, basic goods and primary necessities. For their nature and infrastructure, the flexographic industry is very complex and difficult to replace in case of necessity.

According to [24], this industry is characterized by the use of the Anilox (Rolls engraved with microcells using modern laser technology that is used for the transference of the inks to the substrate) and by other technical processes described in more detail by [25] and [26], making flexography, today, a flourishing and necessary industry for society and the economy due to its neuralgic and essential nature, demonstrated by the past Covid-19 pandemic, which revealed its status as a critical productive infrastructure. As an essential and difficult to replace industry, the flexographic sector faces growing cyber threats due to digitalization, automation and the incorporation of technologies such as DCS, IoT and AI in their production processes and chains.



Fig. 1. Allusion to the flexographic industry and its critical production chain. *Source: Taken from [23].*

4. Materials, methods and research methodology

To solve the question about what a suitable and feasible design of the cybersecurity model for the flexographic industry would be to ensure the confiability, integrity and availability of the computing infrastructure associated to the manage, control and operation of the critical productive line of the flexographic industry was consolidated the ICTBC, cybersecurity model developed through a phased methodology. To this goal, the research effort is structured into three (3) main, successive and articulated phases, aimed to achieve its objectives through a step-by-step approach, ensuring sequential, gradual, and timely results in line with the scientific method. Phase 1 involved a sectoral diagnosis of information security's state, requirements and needs, conducted by applying a diagnostic survey as per the methodologies outlined in [27] and [28]. Phase 2 was realized the depth analysis of the international computer security standards and references, culminating in the consolidation of a cybersecurity prototype. Phase 3, currently in progress, focuses on validating this model through a conceptual test, utilizing a new instrument (a validation survey) applied to an expert focus group, again following the guidelines from [27] and [28].

In this context, was found and considered a cognitive difficulty, it was derived from two (2) transcendental factors was observed: the definition of "model", literally, as a conceptual structure of an abstract character and nature; to which can be added the epistemological obstacle that represented the natural technical complexity of the cybersecurity model for any person no specialized in this field, reasons for which, it was decided to look for a pedagogical and didactic mechanism or tool to facilitate its understanding by C.E.O.s, managers, directors, operators and, in general, people not specialized in computing security.

As a result of the research effort, the McCumber Cube was found in contributions of [10], [11] y [12], which turned out to be ideal to be used as a basis for an engineering innovation process to improve the original McCumber idea [2], in order to solve this cognitive difficulty and facilitate the understanding of the cybersecurity model, devising and creating the cybersecurity model based on the ICTBC framework, whose methodological path based in step by step development process.

5. Found results of the flexographic sectorial's cybersecurity diagnostic

The sectoral diagnosis of the flexographic industry was carried out based on a mixed methodology that combined documentary review with the application of a methodological instrument for information collection (a survey in accordance with and according to the precepts of [27] and [28]), which was directly

applied to companies in the flexographic sector. In this order of ideas, first, national and international reports related to cybersecurity in SMEs were analyzed, as well as official statistics on incidents in the manufacturing industry, to establish a justifying reference. Subsequently, the structured survey that used the Likert scale was designed and applied to technology and production managers from different organizations, including the flexible packaging, labels and corrugated cardboard sectors, in order to identify the level of maturity in information security, the gaps compared to international standards such as ISO/IEC 27001 and NIST 2.0 CSF, and the perception of digital risk in production processes.

Based on the survey results, self-assessments were developed and used as input for the construction of the risk matrix and its corresponding heat map. This allowed for the classification, categorization, and prioritization of the most relevant cyberthreats according to their probability of occurrence and their impact on operations. This procedure visually demonstrated the risk levels in each dimension analyzed, facilitating the prioritization of security controls that were incorporated into the cyber protection prototype and served as input for the design of the ICTBC-based cybersecurity model proposed for the flexographic industry.

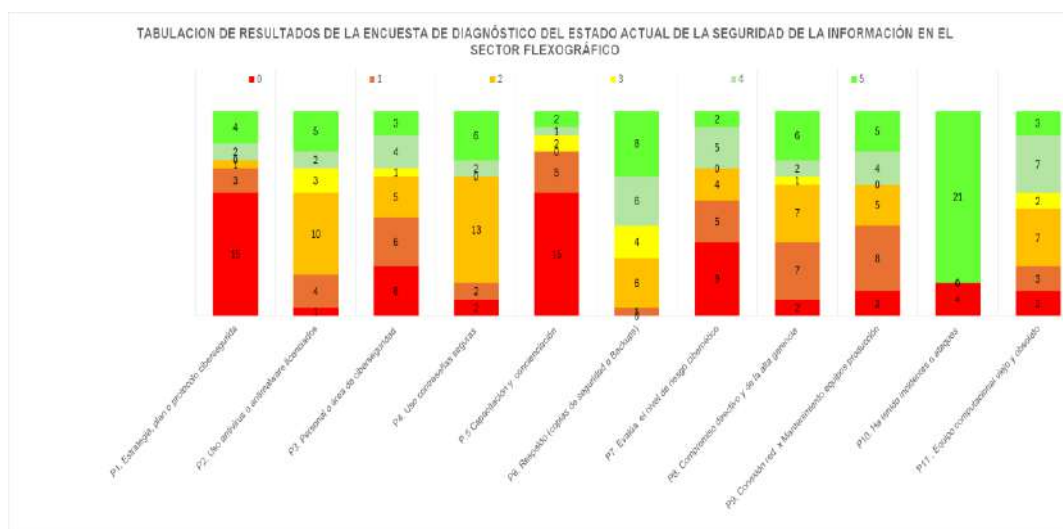


Fig. 2. Bar chart of the results found on the status and cybersecurity needs of the Colombian flexographic industry (2025).

Source: Taken from [23]. Author's work.

The results obtained from the diagnostic survey on the current state of information security in the Colombian flexographic sector reveal a partial and fragmented implementation of key practices. Factors such as inventory, classification, and management of information assets show low levels of maturity, indicating weak management in the identification and protection of critical resources. Similarly, areas such as access control, incident management, and business continuity show a worrying lack of oversight and continuous improvement, which exposes organizations to operational vulnerabilities and limits their ability to respond to cyber-threats (see Fig. 2).

This panorama reveals the urgent need to adopt industrial cybersecurity models that not only respond to technical challenges but also promote a resilient organizational culture. In this sense, the ICTBC framework is positioned as a strategic solution (although still very incipient tool that needs to be refined and polished, like can discuss more ahead). However, ICTBC framework, like useful tool, can contribute to risk reduction, the design and implementation of customized controls, and the consolidation of cyber defense in depth. Its pedagogical approach facilitates the acquisition of complex concepts by non-specialized personnel, which increases the likelihood of effective adoption in diverse production environments.

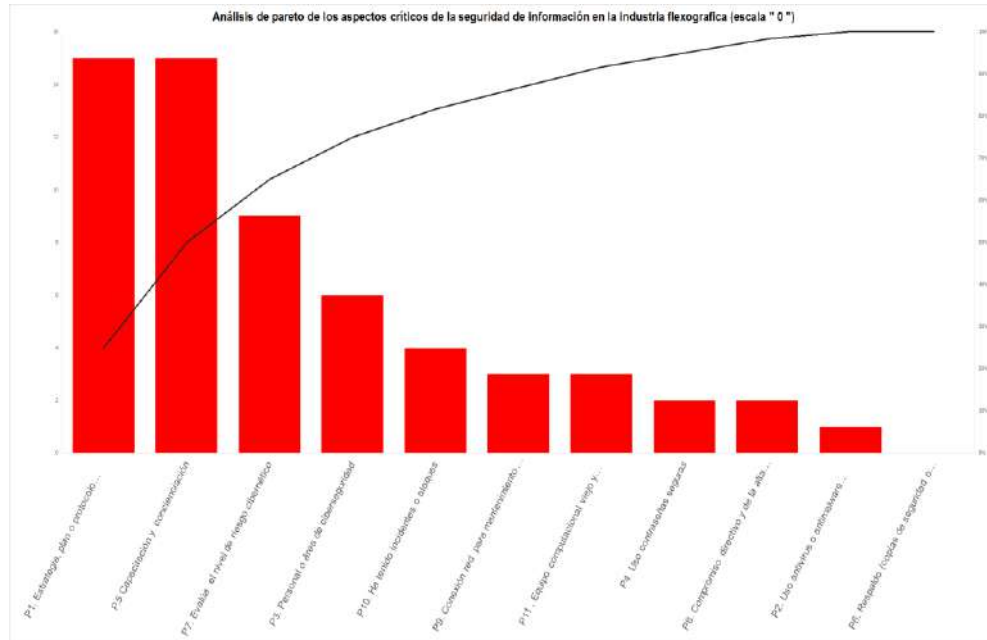


Fig. 3. Pareto analysis of critical information security aspects in the flexographic industry (Security Gaps 2025).
Source: Taken from [23]. Author's work.

The Pareto analysis applied to critical aspects of information security in the flexographic industry reveals a significant concentration of vulnerabilities in key areas such as physical information security, personnel communication and training, and access control. These three factors, at the top of the graph, account for more than 70% of the cumulative impact, indicating that deficiencies in these areas are responsible for most of the operational and technological risks facing the sector. The lack of robust protocols on these fronts compromises the confidentiality, integrity, and availability of digital assets, especially in environments where automation and digitalization are rapidly advancing (see Fig. 3) .

This scenario highlights the need to prioritize corrective and strategic actions in the most critical areas, adopting industrial cybersecurity models that enable structured and adaptable defenses. The ICTBC framework presents itself as a comprehensive solution, offering tools for the design and implementation of customized controls, risk reduction, and strengthening cyber defense in depth. Furthermore, its pedagogical approach facilitates the acquisition of technical concepts by non-specialized personnel, which increases the likelihood of effective and sustained adoption within organizations.

6. Cybersecurity's framework: Industrial Cybersecurity Tinker Bell Cube (ICTBC).

The research effort led to include three (3) new additional dimensions (see Fig. 4) to McCumber original cube [2] like result of considering the particularities and requirements of the industry obtained of the respective risk analysis and evaluation process. In effect, the trends in sophistication, complexity and increase in the quantity and frequency of cyberattacks and their automation, including dangerous tools implemented with AI, usually used by cybercrime groups and organizations, some of them highly specialized in cyberterrorism and cyberwarfare, with a lot of resources (including government support of some countries) and highly trained and technologically advanced are the most current concern for industries. Correspondingly, with the original idea of the McCumber cube, the new dimensions of the ICTBC included

three (3) new categories of security each one, with the intention to operate of similar way of the original cybersecurity cube (see figure 4 with full and complete version of the new ICTBC framework).

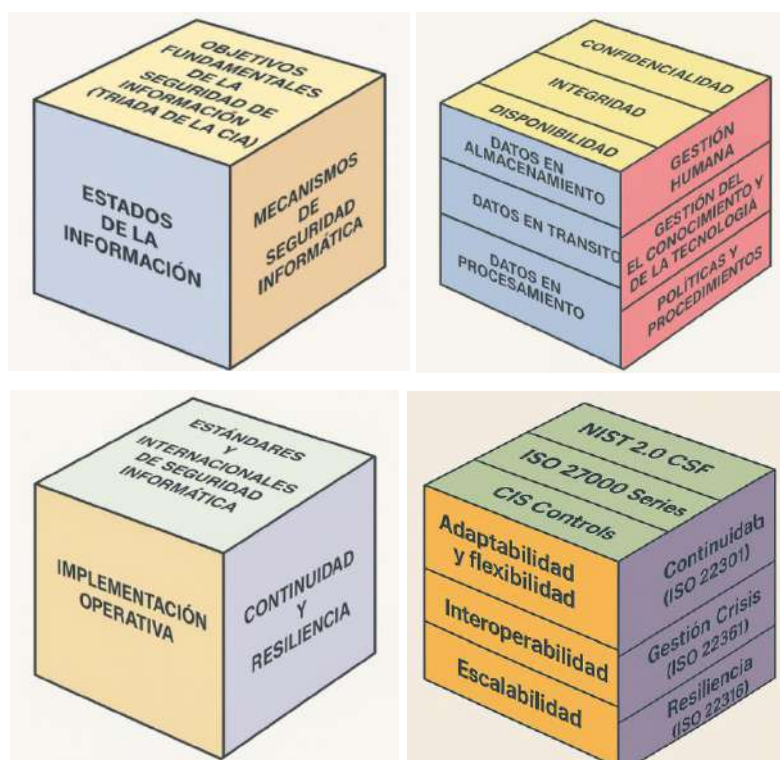


Fig. 4. McCumber's cube (only the two (2) cubes of superior side) and the new Industrial Cybersecurity Tinker Bell Cube (ICTBC) framework (composed by all the cubes of the image, including the McCumber contribution). The image shows all the dimensions and categories of the original cube created by J. R. McCumber (NCSC, 1991) and the new dimensions and categories complemented and enhanced by the authors. *Source: Taken from [3]. Author's work.*

7. Expected Results

Before presenting any results, it is important to clarify that the achievements described here correspond to expected outcomes, as this research is in its development phase and empirical validation of the model has not yet been completed. Therefore, the following constitutes a projection based on theoretical analysis, consideration of the particularities and technical specifications of the industry analyzed, a review of international reference frameworks, and a contextualization of the needs of SMEs in the flexographic sector (potentially applicable to other industries with critical production chains). Consequently, these results should be understood as scoping hypotheses that guide the relevance and applicability of the ICTBC, which may be confirmed, adjusted, or expanded once the pilot implementation is carried out in a company and the corresponding practical evaluations are conducted in real industrial environments.

In any case, it is expected that the implementation of the ICTBC within the cybersecurity model designed for the flexographic industry will achieve concrete and measurable results (including in other productive sectors), in line with the digital protection needs characteristic of SMEs in any essential industry. First, a substantial improvement in cybersecurity maturity is expected, given that organizations will be able

to evolve from a reactive and informal state to the adoption of more structured and proactive practices, supported by international reference frameworks such as ISO/IEC 27001, NIST 2.0 CSF, and CIS Controls.

Another significant expected result relates to the reduction of the level of risk to critical infrastructure. The ICTBC, in its role as a technical tool and mechanism for transmitting cybersecurity concepts, will facilitate the identification of vulnerabilities, the assessment of threats, and the prioritization of mitigation actions. This will reduce the likelihood of cyber incidents disrupting operational continuity or compromising the resilience of production processes. It will also reduce the potential weakness of personnel as the weakest factor or link in the cybersecurity chain by enabling the understanding and assimilation of complex technical concepts of computer security. In this way, cybersecurity will no longer be perceived as an isolated element but will become fully integrated into the operation and protection of the critical production chain, linking risk management with the protection of industrial assets, the supply chain, corporate management systems, and human intervention.

The implementation of the ICTBC will also enable the development of organizational capabilities at various levels. At the technological level, companies will advance measures such as system hardening, network segmentation, monitoring through the adoption of SIEM, and incident response. At the organizational level, corporate policies, awareness programs, and clearly defined responsibilities will be consolidated, with the ICTBC playing an important and significant role in training non-specialized personnel, addressing regulatory requirements, and preparing for emerging threats.

A highly significant expected result and benefit will be the strengthening of continuity and resilience, as organizations will have proven contingency plans, secure backups, and recovery drills that guarantee operational sustainability even in the face of cyberattacks or critical failures. This will be complemented by a greater degree of regulatory compliance and the generation of trust among customers, suppliers, and authorities, which will strengthen corporate reputation within the value chain. Figure 5 shows the cybersecurity model based in ICTBC for the specific case of flexographic industry (see Fig. 5).

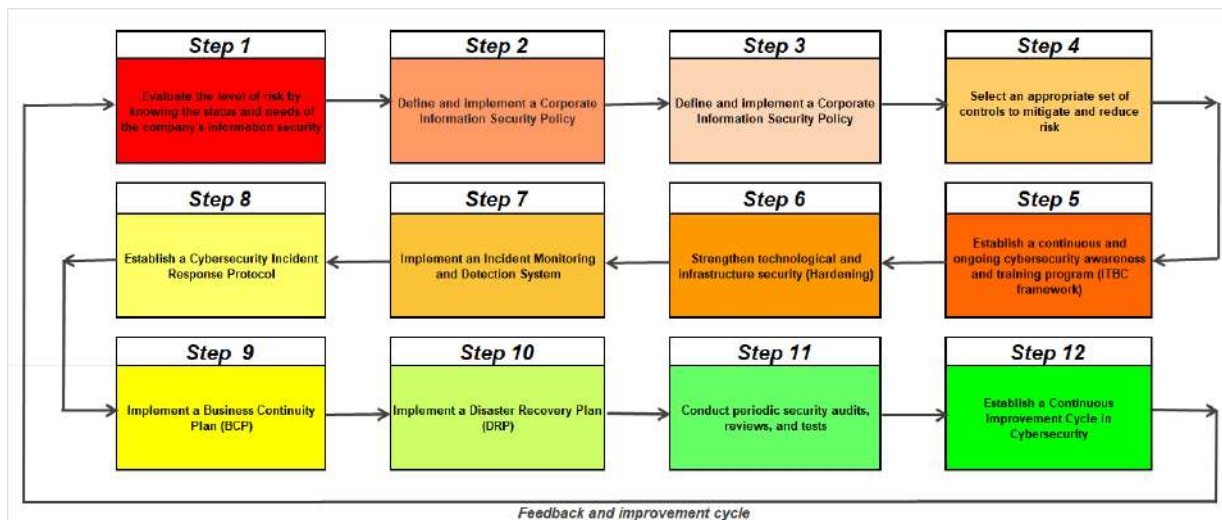


Fig. 5. Cybersecurity model for Flexographic industry based and support in ICTBC. Source: Taken from [3]. Author's work.

Finally, it is worth highlighting once again one of the important aspects expected as a result of incorporating the ITBC as a basic framework for the design of industrial cybersecurity models: in addition to serving as a technical framework, the ITBC will have significant potential as a teaching and training tool

for non-cybersecurity personnel. By translating technical controls into understandable operational practices applicable to the industrial context, the model will become a useful resource for training operators, supervisors, and middle managers. Thus, the CCCI will allow the cybersecurity culture to extend beyond the technological area, ensuring that all personnel acquire basic skills to prevent and respond to incidents, even without advanced technical training.

8. Discussion: ICTBC, a feasible and efficient cyber protection framework and a teaching powerful tool for essential productive sectors and other critical industries

The research developed and materialized in this paper demonstrated that the flexographic industry faces an increasing level of cyber risk due to automation, accelerated digitalization, and the adoption of emerging technologies such as the integration of DCS and the incorporation of IoT and AI into its critical production processes. These circumstances are extendable to other industries with critical production chains and similar characteristics in their productive process. This scenario, coupled with the increasing sophistication, complexity, number, and frequency of cyberattacks, highlights the urgent need to adopt robust cybersecurity models that not only protect IT infrastructure but also guarantee operational continuity and the resilience of critical production chains within this productive sector. These conditions are particularly significant in case of SMEs, more vulnerable and always potential objects to cyberattacks or, inclusive, for another kind of eventualities and circumstances like technical faults, contingences and disasters.

So, the Industrial Cybersecurity Tinker Bell Cube, ICTB represents a methodological engineering innovation process that transcends the traditional ideas of the McCumber Cube's vision of computing security, incorporating new dimensions oriented towards international standards, operational implementation (Adaptability and Flexibility, Interoperability and Integrability, and Scalability, A.I.S.), and an inherent aspect of the industry such as digital continuity and resilience. This conceptual extension not only ensures cyber defense in depth, also responds to a deeply felt pedagogical and didactic need, such as facilitating the understanding of the cybersecurity model by C.E.O.s, managers and non-specialized staff alike, in order to increase the chances of its adoption and success, while simultaneously contributing to strengthening a solid organizational culture of cybersecurity inside of the SMEs and companies of these critical industrial sector.

The implementation of an industrial cybersecurity model based on ICTBC framework is projected to be a key factor in improving the security posture of SMEs, not only in the Colombian flexographic sector, but also, eventually, in other similar critical production sectors. First, a significant reduction in the level of cyber risk is expected through the adoption of controls aligned with international standards and security best practices, based on the various protection options provided by the ICTBC. This will ensure the confidentiality, integrity, and availability of information security in the IT infrastructure associated with the management, operation and control of the critical production chain of SMEs and companies in the sector, supplying continuity and resilience like added value of the cybersecurity model proposed.

Optimization of cybersecurity management is also expected, through clear monitoring, evaluation, and auditing mechanisms that facilitate well-informed strategic decision-making by companies. Another key outcome is the development or strengthening of the organizational cybersecurity culture, driven by the ease of understanding and adoption of the ICTBC by C.E.O.s, managers and non-specialized personnel. This contributes to minimizing human error as a strategy to combat the weakest link in the digital security chain. Finally, a significant improvement in the competitiveness and sustainability of the flexographic industry is

anticipated, given that compliance with robust IT security requirements is increasingly valued in the global industry with critical production chains and in international markets.

9. Clarifications and future research work

Although the paper highlights the pedagogical value of the ICTBC framework as a useful tool for visualizing, appropriating, and applying industrial cybersecurity concepts, also this framework is an very useful tool that can orientate the design of a cybernetic prototype to help to protect the computing systems of an essential industry, without any definitive demerit, because their temporal limitations of validation are acknowledged and will be solutioned with the time in future research works or with some real application derived of the master's thesis. These limitations, visible in this paper, stem from the fact that the work is part of a master's thesis still in progress, and that is primarily focused on protecting the critical production infrastructure of the Colombian flexographic industry.

While the intention of the ICTBC framework is to facilitate understanding among non-specialized audiences—such as operators, middle managers, directors, executives and C.E.O.s—is clearly stated, the thesis does not yet provide a detailed description of the teaching strategies, resources, methodologies, or learning environments required to achieve such appropriation, principally, in reason that the goal of the master's thesis is other, like was consigned before. Each company or future research works about the ICTBC framework's potential and their real implementation can be established to fulfill with this objective. These elements could be addressed in future research within the field of E-Learning or in another master's thesis about ICTBC framework. These suggestions and future development of the ICTBC framework are necessities because is essential issue to solve the absence of instructional guides, simulations, visual materials, participatory dynamics, and feedback mechanisms that currently limits the ability to assess the technical and pedagogical applicability of the ICTBC framework in real-world contexts, such as cyber defense, cybersecurity training, or organizational awareness-building, particularly in SMEs of essential industries and productive sector.

However, from a technical standpoint of cybersecurity, the ICTBC represents a methodological innovation that enables:

- Reduction of cyber risk through targeted identification of vulnerabilities in industrial environments,
- Development and implementation of customized cybersecurity controls tailored to operational realities, particularly, in the specific case of SMEs with critical productive chains,
- Strengthening of in-depth cyber defense by incorporating dimensions such as recognized international standards of computing security and best practices, A.I.S. dimension (adaptation and flexibility, interoperability, and scalability), and the important dimension of digital continuity and resilience,
- Promotion of organizational cybersecurity culture by making the model accessible to non-specialized personnel,
- Integration of engineering, industry, innovation, pedagogy, cybersecurity, and international standards into a comprehensive framework for industrial cybersecurity, like ICTBC.

Without any discussion, the evaluation of the ICTBC's success must be conducted through validation and verification of the efficiency and effectiveness of the cybersecurity model it supports. Given the master's thesis developmental stage, such evaluation should initially be limited to expert focus groups until broader dissemination and adoption allow for more extensive results, first, across the flexographic industry, and, a posteriori, in diverse industrial sectors. So, to reinforce the pedagogical and technical relevance of the ICTBC, future studies should incorporate case analyses, pilot tests, perception surveys, and comparative assessments. These would help demonstrate the framework's impact on learning, adaptation, application, and decision-making processes among both specialized and non-specialized personnel.

Addressing the current methodological and procedural limitations will enable a more robust validation of the innovation of this engineering's process consolidated within the ICTBC. This will provide both technical and pedagogical legitimacy and allow to clarify the degree of understanding and knowledge transfer among end-users and support the creation of metrics and empirical evidence for direct application in industrial environments requiring protection of their critical production chains.

10. Conclusions

The flexographic industry, whose strategic importance became evident during the Covid-19 pandemic, demands a cybersecurity framework capable of enhancing, reinforcing, and evolving the defense-in-depth and cyber protection mechanisms within its SMEs. This necessity arises from the escalating volume, recurrence, complexity, and technical sophistication of cyberattacks, positioning the sector as a growing target for malicious actors seeking to exploit its vulnerabilities.

Throughout the research process, particularly, during the application of a structured methodological framework, unforeseen challenges and contextual demands often emerge that require resolution beyond the scope of the original project design. In the case presented here, one such challenge was the imperative to make a cybersecurity model both visible and comprehensible to organizations within the flexographic industry. This necessity led to the development of the ICTBC, a product of engineering innovation that evolved directly from the expansion, refinement, and enhancement of the McCumber cube for industrial cybersecurity applications.

Importantly, the driving force behind this development was not a purely technical or cybernetic requirement, but rather an educational and cognitive one. The complexity of the cybersecurity model demanded a pedagogical and didactic solution capable of bridging the gap between technical sophistication and organizational understanding. This was essential to ensure its adoption and internalization by managers, executives, and non-specialized personnel across the sector, whose engagement is critical for the successful implementation of cybersecurity strategies in industrial environments.

The McCumber cube remains a pedagogically valuable reference in the field of computer security due to its ability to represent the foundational principles of information security in a structured, three-dimensional format. However, its conceptual scope, shaped over three decades ago, proves insufficient when addressing the complexities of modern cybersecurity, particularly in industrial contexts involving critical production infrastructures and advanced technological environments such as flexographic printing. In response to these limitations, the development of the ICTBC framework through an engineering-driven innovation process offers a technically and pedagogically enhanced alternative. By expanding and adapting the original model, the ICTBC translates complex cybersecurity concepts into a more accessible, applicable,

and educational resource. Its design facilitates understanding and adoption not only among specialized professionals but also among non-expert stakeholders, thereby supporting broader organizational engagement and strengthening cybersecurity culture across industrial sectors.

In practical terms, as an added value of this investigation effort, apart from its contribution to innovation, the cybersecurity model offers a tool that can be replicated in other industrial environments, contributing value to strengthening business competitiveness and sustainability in critical productive sectors. Thus, the ICTBC can come to be, as an effective solution to address current and future cyberthreats, consolidating a comprehensive framework that articulates technology, computer engineering, pedagogy, and innovation to benefit information security in essential industries to the real economy, the country, and society.

11. Recommendations

The following recommendations are the more suitable justification to incorporate the ITBC framework as a very useful tool in cybersecurity. In effect, the main reason is that the adoption of the ICTBC framework isn't only technically justified because their way to operate continue been similar to the original McCumber's cube, but also, very appropriate to a productive environment by its ability to comprehensively address the specific cyber-challenges faced by critical industries in contexts of high automation, digitalization, and exposure to cyberthreats. Unlike traditional approaches limited to the protection of technological infrastructure, the ICTBC incorporates technical, operational and organizational dimensions and the human factor, that enable defense-in-depth, tailored to the realities of industrial SMEs.

From a methodological perspective, the ICTBC facilitates contextualized risk identification, allowing for the mapping of specific vulnerabilities in production processes, digital control systems (DCS), IoT and AI environments, and is an advantage their modular structure allows for the design and implementation of customized controls aligned with each organization's operational and technological capabilities, increasing the efficiency of protective measures without generating technical overload, can be used like a strong base to design particular cybersecurity models highly personalized for specific industries with critical productive chains, like the flexographic sector.

Furthermore, the model promotes the strengthening of the organizational culture in cybersecurity by integrating pedagogical elements that facilitate the understanding and appropriation of the framework by non-specialized personnel. This not only improves internal adoption but also contributes to the sustainability of protection strategies over time. Finally, the ICTBC articulates international standards with local practices, offering a scalable, interoperable, and flexible solution that responds to the technical, regulatory, and operational requirements of contemporary industrial cybersecurity.

12. Acknowledgments and authors profiles

The authors express their gratitude to:

Serviflex Arco Internacional S.A.S. (sponsoring company); Colombian Flexographic industry; Metropolitan Technological Institution (I.T.M.) of Medellín; Jaime Isaza Cadavid Colombian Polytechnic (P.C.J.I.C.) of Medellín; the Agency for Higher Education of Antioquia (Sapiencia); Nacional University of Colombia, Medellín Branche, National Faculty of Mines(UNALMED); University of Antioquia (UdeA); University of Medellín (UdeM); Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC); Integrated Development Center (CENDI); EAFIT University; U.P.B. University; Pascual Bravo University Institution; to our teachers: Eng. Héctor

Fernando Vargas Montoya; Eng. Francisco Eugenio López Giraldo; Eng. Juliver Gil Herrera; Eng. Leonel Marín Ramirez; Eng. Sergio A. Álvarez G.; Eng. Juan F. Puerta Grajales; Eng. Andres Alberto Gómez Acosta; Eng. Alex Mauricio Ávila Quiceno; Eng. Héctor Valencia Valencia; Eng. Fredy Humberto Gómez Orjuela; Eng. Hernán Francisco Villar Vega; Eng. Julián Andrés Naranjo Londoño; Eng. Jorge Ernesto Espinosa Oviedo; Eng. Sixto Enrique Campaña Bastidas; Eng. Juan Carlos Rodríguez Gamboa; Eng. Miguel Ángel Roldán Álvarez; Eng. Joel Carroll Vargas; Eng. Andres Felipe Aristizábal Durango; to our director's staff: Lawyer Alejandro Villa Gómez (I.T.M.'s Rector); Eng. Eduard Alberto García Galeano (ITM's Financial Vicerrector); Eng. Carlos Julio Escobar Noreña (Postgrade's Chief); Eng. Olga Lucía Henao Pardo (Dean of Engineering Faculty, PCJIC); Eng. Adriana Xiomara Reyes Gamboa (ITT's Doctoral program, PCJIC); Eng. Gladis Helena Vásquez Echavarría (Director of ADV specialization program, PCJIC); to our colleagues: Eng. Francisco Antonio Gutiérrez Calderón (ITM); Eng. Orlando Villabona Bolaños (ITM); Eng. Aixa Eileen Villamizar Jaimes (TdeA). Also, the authors thank CISCO; IBM; Google (YouTube); Microsoft; OpenAI; AWS; and all the various YouTubers of cybersecurity and related fields for providing access to E-Learning resources and technological tools used in the develop of the graduate programs of cybersecurity specialization and magister in computer security (ITM), particularly, to help us in our ethical hacking formation way and to elaborate of our magister's thesis and to consolidate this innovative research (ICTBC).

About the authors:

¹ **Eng. Edgar Alberto Acevedoarango.**

Electrical Engineer (National University of Colombia, National Faculty of Mines, Medellín); Magister's Degree in Business Administration – M.B.A. (EAFIT University); Specialist's degree in International Business (EAFIT University); Specialist's degree in Cybersecurity (U. I.T.M.); Magister's Degree candidate in Computing Security (c) (U. I.T.M.); Specialist's degree candidate in Data Analytics (c) (Jaime Isaza Cadavid Colombina Polytechnic University).

Member 101531609 of the Institute of Electrical and Electronics Engineers (IEEE); member 2202483 of Information Systems Audit and Control Association (ISACA); member 27575645 of the SANS Institute; member 2854043 of Open Worldwide Application Security Project (OWASP); member of Rivest, Shamir & Adleman Conference (RSAC); member 27575645 of The Association for the Advancement of Artificial Intelligence (AAAI); member of International Association for Safe & Ethical Artificial Intelligence (IASAI); member 429164 of International Council on Systems Engineering (INCOSE) - Artificial Intelligence Systems, Critical Infrastructure Protection and Recovery and Systems Engineering for Industrial Systems communities of LatAm Chapter -; member 2949019 of International Information Systems Security Certification Consortium ((ISC)2) (c); member 1122027569 of the Institution of Engineering and Technology of United Kingdom (IET SSO, UK); member of Asociación Internacional de Ciberseguridad (ASICI); member of Centro de Ciberseguridad Industrial (CCI); member 2343187 of Internet Society (ISOC); member of Blockchain Council (BCC); member of Asociación Colombiana de Ingenieros (ACIEM) (c); member of Sociedad Colombiana de Computación (SCO2); member of Asociación de Ingenieros Egresados de la Facultad Nacional de Minas (ADEMINAS UNALMED); and member of ResearchGate. ORCID: <https://orcid.org/0009-0001-1339-0517>. Manager of Innovation, Projects, R&D, and New Technologies. Serviflex Arco Internacional S.A.S. Medellín, Antioquia, Colombia. Contact: ea.researcher@gmail.com –

² **Eng. Adriana María Echeverri Londoño.**

Chemical Engineer (University of Antioquia); Magister's Degree in Business Administration – M.B.A. (EAFIT University); Specialist's Degree in Quality Management (EAFIT Univ.); Specialist's degree in Cybersecurity (U. I.T.M.); Magister's Degree candidate in Computing Security (c) (U. I.T.M.).

Member 101531882 of the Institute of Electrical and Electronics Engineers (IEEE), member 2202484 of Information Systems Audit and Control Association (ISACA), member 30398330 of SANS Institute, member 2854045 of Open Worldwide Application Security Project (OWASP), member of Rivest, Shamir & Adleman Conference (RSAC), member 429167 of International Council on Systems Engineering (INCOSE) - Critical Infrastructure Protection and Recovery, Resilient Systems, and Systems Engineering Quality Management (SEQM) communities of LatAm Chapter -; member 2949063 of International Information Systems Security Certification Consortium ((ISC)2) (c); member of Cybersecurity International Association (ASICI); member of Centro de Ciberseguridad Industrial (CCI); member 2343188 of Internet Society (ISOC); member 1122027570 of the Institution of Engineering and Technology of United

Kingdom (IET SSO, UK); member of Blockchain Council (BCC); member of Asociación Colombiana de Ingenieros (ACIEM) (c); and member of the Sociedad Colombiana de Computación (SCO2); and member of ResearchGate.
ORCID: <https://orcid.org/0009-0002-4525-076X>.
Commercial, Technical & Computing Security Manager. Serviflex Arco Internacional S.A.S. Medellín, Ant., Colombia. Contact: ameltempo1212@gmail.com



Fig. 6. The ICTBC's creators and authors of this paper (Eng. Edgar Alberto Acevedoarango and Eng. Adriana María Echeverri Londoño). Source: Taken from [3].

13. References and bibliography

- [1] **Mejía Cortez, E.M.:** El mercado de la flexografía en Latinoamérica. Revista Coyuntura Económica, Instituto de Investigaciones Económicas, San Salvador, El Salvador (2024). Disponible en: <https://revistas.ues.edu.sv/index.php/coyunec/article/download/423/355>
- [2] **McCumber, J.R.:** Information Systems Security: A Comprehensive Model. In: Proc. 14th National Computer Security Conference, NIST/NCSC, Washington, D.C., USA, pp. 328 –337 (1991). Disponible en: <https://csrc.nist.gov/files/pubs/conference/1991/10/01/proceedings-14th-national-computer-security-confer/final/docs/1991-14th-ncsc-proceedings-vol-1.pdf>
- [3] **Acevedoarango, E.A., Echeverri L., A.M.:** Diseño de un modelo de ciberseguridad para la cadena de producción crítica de la industria flexográfica. Tesis de Maestría en Seguridad Informática, ITM, Medellín, Colombia (2025). Disponible en: www.serviflexarco.com
- [4] **Dini, M., Stumpo, G.:** MIPYMES en América Latina. Un frágil desempeño y nuevos desafíos para las políticas de fomento. Naciones Unidas, Santiago de Chile, Chile (2020). Disponible en: <https://repositorio.cepal.org/server/api/core/bitstreams/2c7fec3c-c404-496b-a0da-e6a14b1cee48/content>
- [5] **Bautista Chimarro, F.F., Flores Ruiz, A.E., Aguirre Inga, R.G.:** Ciberseguridad en PYMEs: Caso de estudio en Cayambe. Revista Científica Dominio de las Ciencias 9 (4), 388–402 (2023). Disponible en: <https://dominiodelasciencias.com/ojs/index.php/es/article/view/3597/7875>
- [6] **Kamlosfsky, J., Colombo, H.R., Sliafertas, M.N., Pedernera Gaitán, J.M.:** Un enfoque para disminuir los efectos de los Ciber-ataques a las Infraestructuras Críticas. Sistema Pedagógico Vaneduc (SPV) (2015). Disponible en: <https://imgbiblio.vaneduc.edu.ar/fulltext/files/TC121046.pdf>
- [7] **Quintana, J., Cornejo, F., Rigail Cedeño, A.:** Análisis y Diseño de Empaques Flexibles para Alimentos. Revista Tecnológica ESPOL 20(1), 11–18 (agosto-octubre de 2007). Disponible en: <https://rte.espol.edu.ec/index.php/tecnologica/article/view/156/100>
- [8] **Acevedoarango, E.A.:** Sistemas de Control Digital en Subestaciones Eléctricas de Alta y Extra Alta Tensión. Tesis de Ingeniería Eléctrica, Universidad Nacional de Colombia, Medellín, Colombia (1997). Disponible en: www.serviflexarco.com

- [9] **Guaña-Moya, J.:** Revolución de la ciberseguridad en la cuarta revolución industrial. Revista Ingeniería e Innovación del Futuro 2(2) (julio-diciembre de 2023). Disponible en: <https://editorialscientificfuture.com/index.php/riif/article/view/11/13>
- [10] **Millà, A.:** McCumber Cube (El cubo). Blog de Alex Millà (1 de mayo de 2023). Disponible en: <https://alexmilla.net/seguridad/mccumber-cube-el-cubo>
- [11] **Pampliega, E.:** ¿Qué es el Cubo de McCumber? Un mundo complejo/TIC/Ciberseguridad (2023). Disponible en: <https://epampliega.com/blog/index.php/2023/09/07/que-es-el-cubo-de-mccumber/>
- [12] **Guzmán Mercado, R.B.:** The McCumber Cube and Cybersecurity (2023). Disponible en: <https://www.rberny.com/2023/06/08/el-cubo-de-mccumber-y-la-ciberseguridad/>
- [13] **ISO:** Norma ISO/IEC 27001:2022 (2022). Disponible en: <https://www.iso.org/es/home>
- [14] **OEA, AWS:** Ciberseguridad marco NIST: Un abordaje integral de la ciberseguridad, 5th ed. (2019). Disponible en: <https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf>
- [15] **Dávila Fernández, M.C., Muñoz Huaman, J.:** Diseño de controles de ciberseguridad para reducir los ciberataques en empresas distribuidoras de productos digitales basados en CIS control V8. Tesis de Pregrado, Univ. Peruana de Ciencias Aplicadas, Lima, Perú (2023). Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/670133/Davila_FM.pdf
- [16] **ISO:** Norma ISO 22301:2019 (2019). Disponible en: <https://www.iso.org/es/home>
- [17] **ISO:** Norma ISO 22361:2022 (2022). Disponible en: <https://www.iso.org/es/home>
- [18] **ISO:** Norma ISO 22316:2017 (2017). Disponible en: <https://www.iso.org/es/home>
- [19] **Castiblanco, F., Oviedo Regueros, L.A.:** Análisis de riesgos informáticos y sugerencia de controles para la mitigación del riesgo empleando las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005. Trabajo de Grado, Univ. Nacional Abierta y a Distancia, Bogotá, Colombia (2017). Disponible en: <https://repositorio.unipiloto.edu.co/bitstream/handle/20.500.12277/2660/Trabajo%20de%20grado.pdf>
- [20] **Hurtado Rivera, J.F.:** Curso de introducción a la ciberseguridad. Instituto Tecnológico Metropolitano (ITM), Medellín, Colombia (2024). Disponible en: <https://campusvirtual.itm.edu.co/login/index.php>
- [21] **Álvarez Gaviria, S.A.:** Curso de Redes y Ciberseguridad. Univ. de Antioquia, Medellín, Colombia (2024). Disponible en: <https://ingenia.udea.edu.co/>
- [22] **Acevedoarango, E.A., Echeverri L., A.M.:** ICTBC : pedagogical and didactic strategy to facilitate the understanding of an industrial cybersecurity model based on an innovative engineering process through the conceptual expansion of the ‘McCumber cube’. In: XX Conf. Latinoamericana de Tecnologías de Aprendizaje (LACLO), Medellín, Colombia (2025). Disponible en: <https://marca.tdea.edu.co/laclo/llamado.php>
- [23] **Envapack.com:** Planta de Establecimiento Gráfico con Cadena de Producción de última generación (Bobst) (2024). Disponible en: <https://www.envapack.com/2019/05/establecimiento-grafico-impresores-continua-creciendo-en-el-mercado-de-embalaje-flexible-con-impresoras-flexo-de-tambor-central-y-maquinas-laminadoras-bobst/>
- [24] **Acevedoarango, E.A., Echeverri L., A.M.:** Libro Gordo del Anilox: Breviario de fundamentos para optimizar la utilización, desempeño y duración de los Anilox, 2nd ed. Serviflex Arco Internacional S.A.S., Medellín, Colombia (2017). Disponible en: www.serviflexarco.com
- [25] **Acevedoarango, E.A.:** Aplicación de los fenómenos electromagnéticos en la industria convertidora. Revista Mundo Eléctrico 17(65) (2009). Disponible en: <https://www.mundoelectrico.com/edicion-n-65-20-anos>
- [26] **Acevedoarango, E.A., Echeverri L., A.M.:** Libro Gordo del Tratamiento Corona: Breviario de ideas fundamentales sobre tratamiento superficial corona en flexografía y conversión, 3rd ed. Serviflex Arco Internacional S.A.S., Medellín, Colombia (2017). Disponible en: www.serviflexarco.com
- [27] **Hernández Sampieri, C.R., Fernández Collado, C., Baptista Lucio, P.:** Metodología de la investigación. McGraw-Hill, Naucalpan, México (1991). Disponible en: <https://www.academia.edu/102204834/>
- [28] **Casas Anguita, J., Repullo Labrador, J.R., Donado Campos, J.:** La encuesta como técnica de investigación. Revista Atención Primaria 31(8), 527–538 (2003). Disponible en: <https://core.ac.uk/download/pdf/82245762.pdf>

Anexo Nro. 14

**Productos de esta de esta tesis de maestría
en seguridad informática.**

**Participaciones, cursos y eventos.
Certificaciones obtenidas en eventos,
cursos y capacitaciones realizados durante
y para el desarrollo de esta investigación de
tesis de maestría en seguridad informática.**

Ver archivo PDF a continuación

Instituto Tecnológico Metropolitano – I.T.M. – Maestría en Seguridad Informática

Diseño de un modelo de ciberseguridad para la cadena
productiva crítica de la industria flexográfica

Edgar Alberto Acevedoarango y Adriana María Echeverri Londoño

FASE 4 y FASE 5



Certificate no: UC-ed90623-6820-4bc8-94ac-50b79ce635ec

Certificate url: ude.my/UC-ed90623-6820-4bc8-94ac-50b79ce635ec

Reference Number: 0004

CERTIFICATE OF COMPLETION

Implementando NIST Cybersecurity Framework 2.0 (CSF)

Instructors **Fernando Conislla Murguia**

Edgar Alberto Acevedoarango

Date **March 10, 2025**

Length **4 total hours**



Certificate no: UC-c16fdf14-b4f8-40ae-86f4-949c35e9dcfc
Certificate url: ude.my/UC-c16fdf14-b4f8-40ae-86f4-949c35e9dcfc
Reference Number: 0004

CERTIFICATE OF COMPLETION

Implementando NIST CSF 2.0

Instructors **Fernando Conislla Murguia**

Adriana Echeverri

Date **Feb. 22, 2025**

Length **4 total hours**



UNIVERSIDAD MILITAR
NUEVA GRANADA

10, 11, y 12 de SEPTIEMBRE



CONGRESO
COLOMBIANO
DE COMPUTACIÓN
COMPUTACIÓN PARA ENTORNOS
MÁS SOSTENIBLES

La Universidad Militar Nueva Granada certifica que:

El trabajo titulado,

"ICTBC (CCCI): ENGINEERING INNOVATION PROCESS APPLIED IN THE DESIGN OF AN INDUSTRIAL CYBERSECURITY MODEL BY IMPROVING THE MACCUMBER CUBE",

realizado por

ACEVEDOARANGO, EDGAR ; ECHEVERRI LONDOÑO, ADRIANA MARÍA

fue presentado en la modalidad de ponencia oral en el

19 Congreso Colombiano de Computación – 19CCC

Ing. Wilson Javier Sarmiento Manrique
Presidente comité académico 19CCC

Ing. Wilfrido Arteaga Sarmiento
Decano Facultad de Ingeniería

Inf. Eduard Leonardo Sierra Ballén
Presidente comité directivo 19CCC

SCO² SOCIEDAD COLOMBIANA
DE COMPUTACIÓN

**INGENIERÍA
EN MULTIMEDIA**





LACLO 2025
COLOMBIA

The work

**ICTBC (CCCI): PEDAGOGICAL AND DIDACTIC STRATEGY TO
FACILITATE THE UNDERSTANDING OF AN INDUSTRIAL
CYBERSECURITY MODEL BASED ON AN INNOVATION ENGINEERING
PROCESS THROUGH THE CONCEPTUAL EXPANSION OF THE
“MACCUMBER CUBE”**

Developed by

ACEVEDO ARANGO, EDGAR; ECHEVERRI LONDOÑO, ADRIANA MARÍA

was presented at **LACLO 2025 - Latin American Conference of Learning Technologies** ,
in Medellín, Colombia, from November 4 to 7, 2025, in the Paper section.


DARIO ENRIQUE SOTO DURÁN
General Chair
Tecnológico de Antioquia


ADRIANA XIOMARA REYES GAMBOA
General Chair
Politécnico Jaime Isaza Cadavid

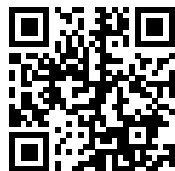
Certificate of Course Completion

EDGAR ALBERTO ACEVEDOARANGO

has successfully achieved student level credential for completing the Networking Basics course.

The student was able to proficiently:

- Explain important concepts in network communication, network types, components, and connections.
- Explain the importance of standards and protocols in network communications.
- Explain how communication occurs on Ethernet networks.
- Explain the features of an IP address and IPv4 addresses are used in network communication.
- Explain features of IPv6 addressing.
- Explain how routers connect networks together.
- Use various tools to test and troubleshoot network connectivity.
- Configure an integrated wireless router and wireless client to connect securely to the internet.



Scan to Verify

Laura Quintana

Laura Quintana
Vice President and General Manager
Cisco Networking Academy

February 07, 2024

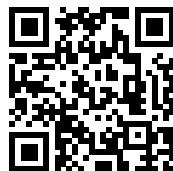
Certificate of Course Completion

ADRIANA MARÍA ECHEVERRI LONDOÑO

has successfully achieved student level credential for completing the Networking Basics course.

The student was able to proficiently:

- Explain important concepts in network communication, network types, components, and connections.
- Explain the importance of standards and protocols in network communications.
- Explain how communication occurs on Ethernet networks.
- Explain the features of an IP address and IPv4 addresses are used in network communication.
- Explain features of IPv6 addressing.
- Explain how routers connect networks together.
- Use various tools to test and troubleshoot network connectivity.
- Configure an integrated wireless router and wireless client to connect securely to the internet.



Scan to Verify

Laura Quintana

Laura Quintana
Vice President and General Manager
Cisco Networking Academy

February 05, 2024

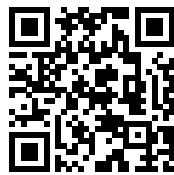
Certificate of Course Completion

EDGAR ALBERTO ACEVEDOARANGO

has successfully achieved student level credential for completing the Introduction to Cybersecurity course.

The student was able to proficiently:

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect oneself while online.
- Explain how organizations can protect their operations against these attacks.
- Access a variety of information and resources to explore the different career options in cybersecurity.



Scan to Verify

Laura Quintana

Laura Quintana
Vice President and General Manager
Cisco Networking Academy

November 11, 2023

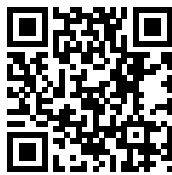
Certificate of Course Completion

ADRIANA MARÍA ECHEVERRI LONDOÑO

has successfully achieved student level credential for completing the Introduction to Cybersecurity course.

The student was able to proficiently:

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect oneself while online.
- Explain how organizations can protect their operations against these attacks.
- Access a variety of information and resources to explore the different career options in cybersecurity.



Scan to Verify

Laura Quintana

Laura Quintana
Vice President and General Manager
Cisco Networking Academy

November 14, 2023



Institución Universitaria

Medellín, 12 de Diciembre de 2025.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años



DISEÑO DE UN MODELO DE CIBERSEGURIDAD PARA LA CADENA PRODUCTIVA CRÍTICA DE LA INDUSTRIA FLEXOGRÁFICA





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años

Diseño de un modelo de ciberseguridad para la cadena productiva crítica de la industria flexográfica

Trabajo de Grado o Tesis de Maestría en *Seguridad Informática*

Por:

Ing. **Edgar Alberto Acevedoarango**

y

Ing. **Adriana María Echeverri Londoño**

INSTITUTO TECNOLÓGICO METROPOLITANO - ITM

Maestría en Seguridad Informática

Medellín, 07 de Abril de 2026.





Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

Agenda

1 – Motivación y contexto	6 – Resultados
2 – Descripción del problema, Alcance	7 – Conclusiones y recomendaciones
3 – Antecedentes, trabajos previos y justificación	8 – Trabajos Futuros
4 – Objetivos	9 – Productos
5 – Metodología de investigación	10 – Referencias
	11 – Agradecimientos



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

1

Motivación y contexto



Motivación:

En gratitud a la industria flexográfica, por más de dos décadas de trabajo y sustento, se desea dejar un legado útil que contribuya a mejorar la seguridad informática sectorial y, en particular, la ciberdefensa de sus PYMEs.



La industria Flexográfica:

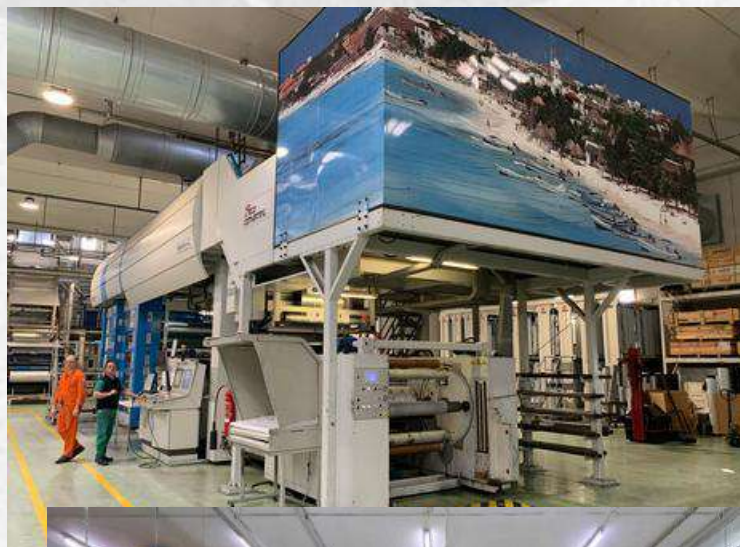
- La industria flexográfica es la que tiene como finalidad realizar la impresión, utilizando planchas flexibles en relieve para transferir tinta directamente, en una amplia variedad de materiales, incluidos plásticos, papel, cartón, aluminio, entre otros. Destacando por su versatilidad, rapidez y costos eficientes en tiradas medias y largas.
- Compuesta por sectores como banda ancha y empaques flexibles, banda angosta y etiquetas, cartón corrugado, esta en permanente proceso de digitalización y automatización. Se trata de un sector industrial esencial, como lo demostró la pasada pandemia de Covid-19.





Institución
Universitaria | 80
Reacreditada en Alta Calidad | Años

La industria flexográfica



Contexto



- Entorno cibernético plagado de amenazas cada vez más frecuentes, sofisticadas, complejas y de crecimiento exponencial.
- En la actualidad, la industria flexográfica y, en particular, sus PYMEs, constituyen blancos de interés para ciberataques.
- Ya no se trata de si te van a atacar o no, sino, de cuando te van a atacar.





Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

2

Descripción del Problema, Alcance



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

Descripción del Problema

La problemática investigada se consolida en la vulnerabilidad de la infraestructura TI que soporta la gestión de la cadena de producción del sector flexográfico, la cual enfrenta un proceso de digitalización acelerado sin contar con marcos de protección adecuados a su realidad, condiciones y recursos, particularmente, en el caso de las PYMEs.

La brecha digital peligrosa por la carencia de estrategias de ciberseguridad personalizadas, prácticas y adaptables, donde la complejidad de los estándares internacionales y las limitaciones presupuestarias incrementan la exposición de infraestructura TI ante ciberataques e incidentes.



Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años

Alcance

- El alcance de este trabajo de grado está exclusivamente circunscrito a la infraestructura TI que soporta la gestión de la cadena de producción de la industria flexográfica.
- La infraestructura OT se deja para un trabajo futuro, a fin de completar el modelo de ciberseguridad aquí propuesto.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

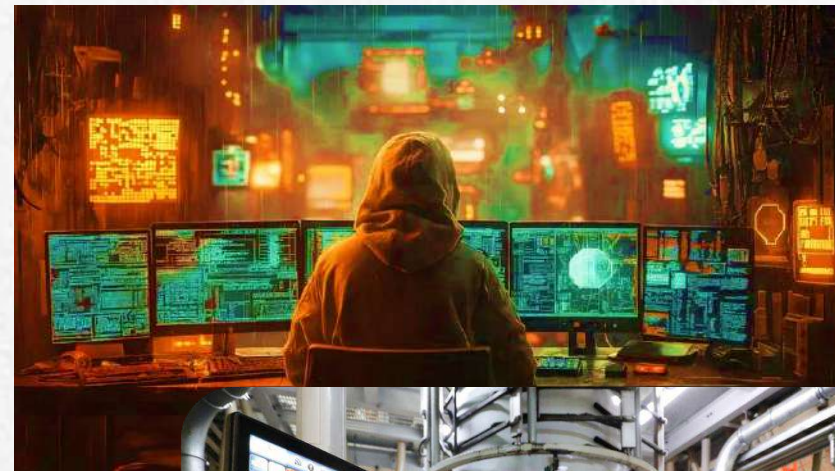
3

Antecedentes y trabajos previos



Antecedentes

- Entorno cibernético con amenazas sofisticadas y frecuentes.
- Bajo enfoque preventivo y proactivo de los activos críticos de producción y la información.
- Bajo índice de capacitación, brecha pedagógica.
- Carencia de modelos de ciberseguridad prácticos, adaptables para proteger TI según necesidades de PYMEs.

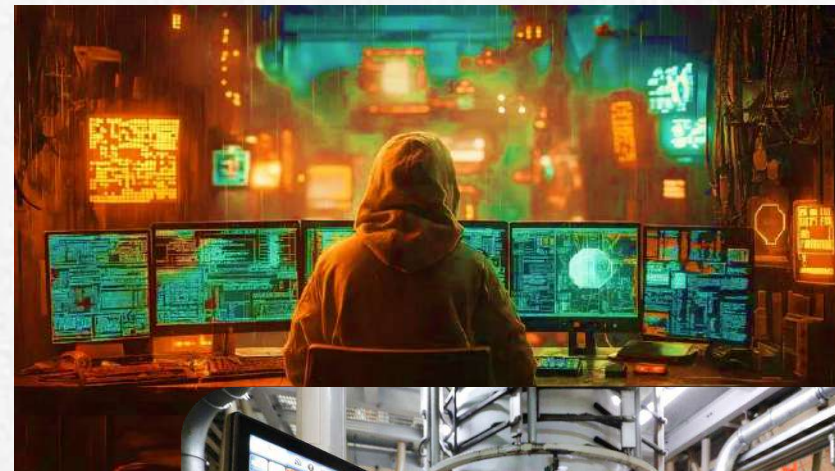


Trabajos previos

El estado del arte reveló desarrollos en muchos tipos de sectores, como:

- Bancario y financiero
- Energético (Sector Eléctrico y sector Gas)
- Sanitario y de salud
- Servicios Tecnológicos
- Textil y manufacturero
- Gubernamental (Educación, Municipios, etc.)

Primer trabajo en la industria flexográfica



Costos de los tipos de Incidentes



Justificación

Costo promedio de ataques cibernéticos por tamaño de empresa (ACIS, 2025)



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

4

Objetivos



Objetivo General



Proponer el diseño de un modelo de ciberseguridad, basado en estándares internacionales y buenas prácticas de seguridad, que permita la conservación de la confidencialidad, integridad y disponibilidad de los sistemas informáticos asociados a los procesos productivos críticos de una PYME del sector flexográfico.

Objetivos Específicos

- Identificar el estado actual y las necesidades y requerimientos de seguridad de la información del sector flexográfico.
- Caracterizar los elementos aplicables de los estándares internacionales seleccionados y de las buenas prácticas de seguridad informática para la consolidación del diseño del modelo de ciberseguridad propuesto.
- Validar el modelo de ciberseguridad mediante una prueba de concepto.





Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

5

Metodología de investigación



Metodología de investigación

El método utilizado se realizó por fases y a cada objetivo específico le correspondió una fase.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

Metodología de investigación

FASE 1: Diagnóstico Sectorial

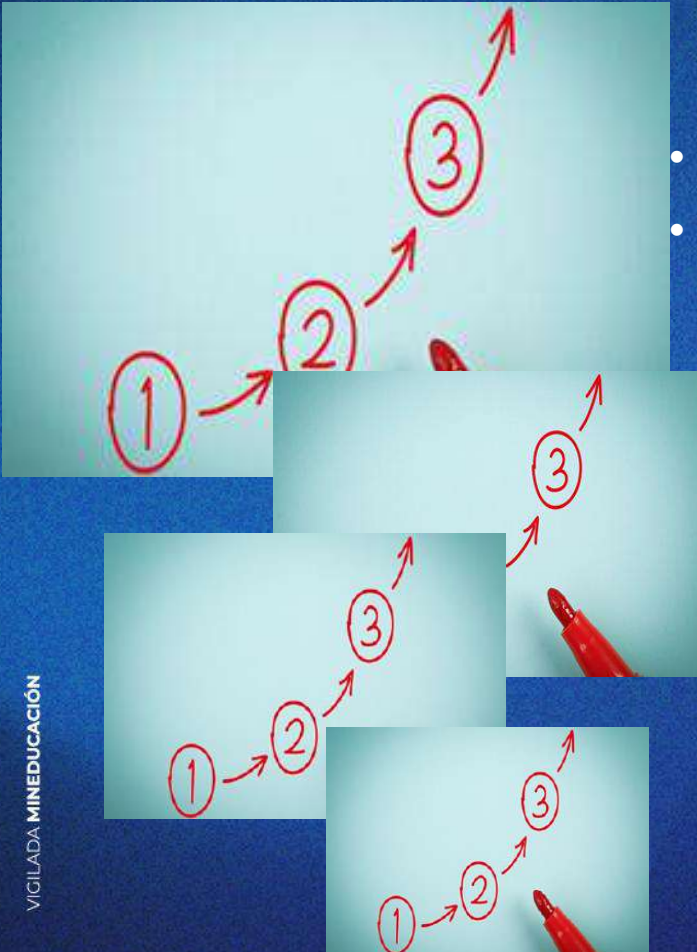
Actividad:

Instrumento aplicado:

Encuesta de Diagnóstico Sectorial de SI

Producto:

Análisis y evaluación de riesgo informático de la infraestructura TI con su respectiva matriz de riesgo y mapa de calor.



Metodología Investigativa

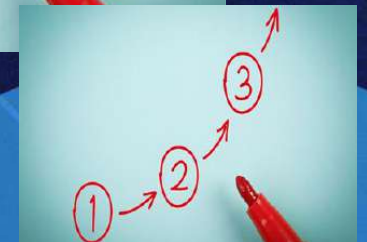
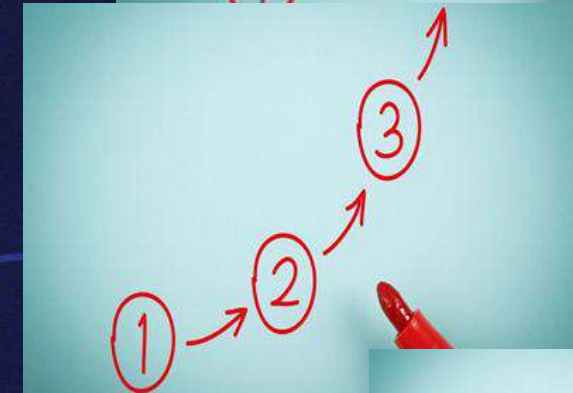
- **FASE 2: Análisis de estándares y referentes de SI y consolidación del modelo de ciberseguridad**

Actividad: Revisión y análisis de estándares

Producto: Selección de controles

Actividad: Diseño prototipo cibernético protectivo

**Productos: Modelo de ciberseguridad
Nuevo marco CCCI (ITBC)**





Metodología Investigativa

- **FASE 3: Verificación del modelo de ciberseguridad**

Actividad:

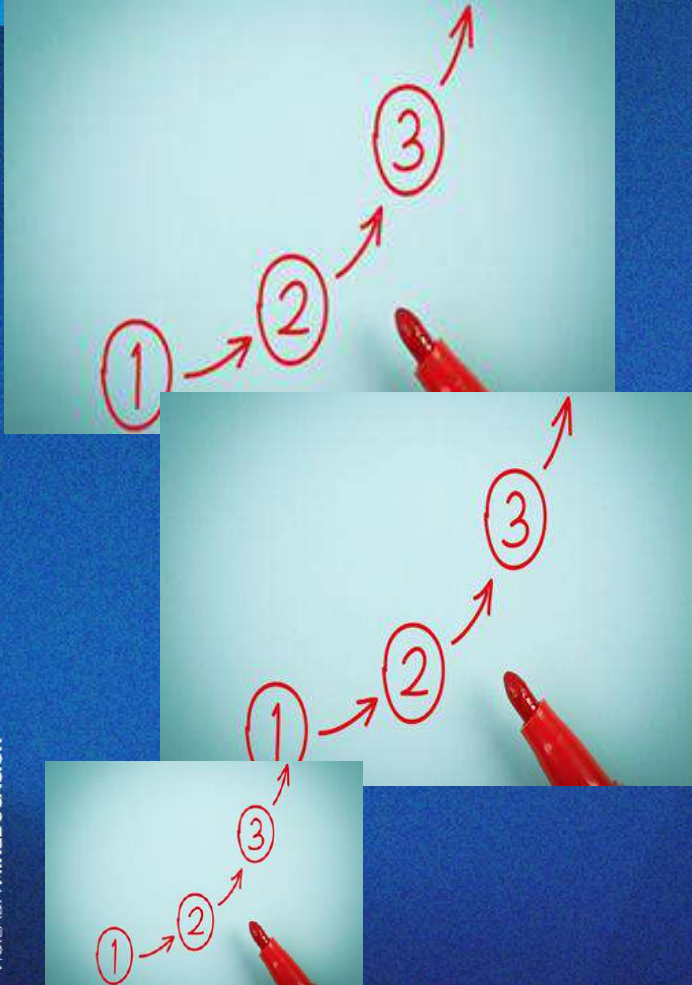
Validación por prueba conceptual.

Instrumento:

Encuesta final.

Producto:

Verificación del prototipo cibernético protectivo.





Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

6

RESULTADOS

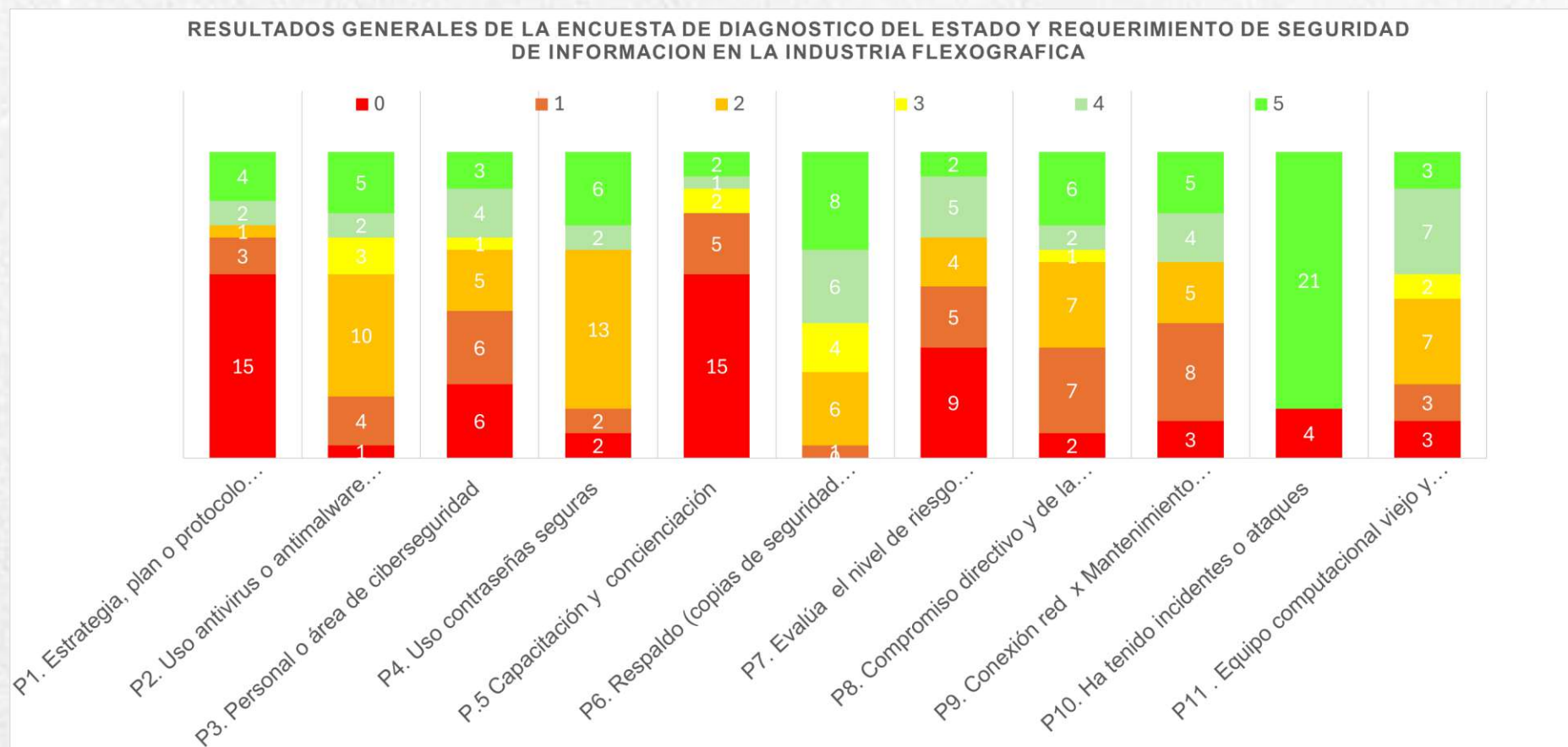


Fase 1: Diagnóstico sectorial de SI en la industria flexográfica

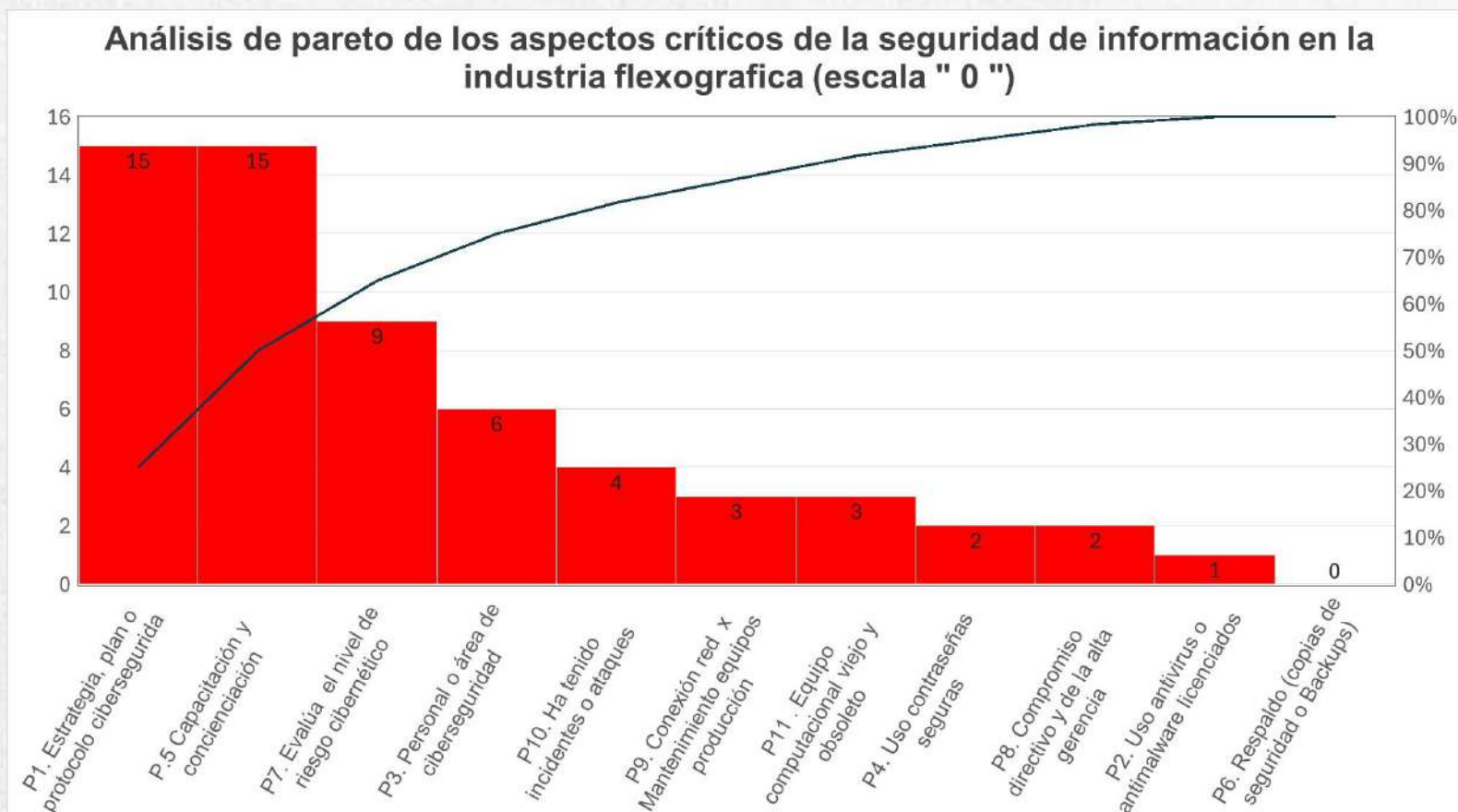
PREGUNTA NRO.	CUESTIONAMIENTO / PREGUNTA
1	¿Su empresa cuenta con una estrategia, plan o protocolo de ciberseguridad o de manejo de incidentes cibernéticos, formalmente implementado, que asegure la confiabilidad, integridad y disponibilidad de sus sistemas y equipos informáticos, en especial los de su cadena de producción?
2	¿Su empresa tiene formalmente implementadas medidas de seguridad , como antivirus o antimalware licenciados, para proteger los sistemas informáticos y la información corporativa contra amenazas maliciosas, como ataques cibernéticos?
3	¿Su empresa cuenta con personal o un departamento de ciberseguridad que asegure la confiabilidad, integridad y disponibilidad de su infraestructura y equipos informáticos, en especial los de su cadena de producción?
4	¿Existen controles , como contraseñas seguras con factor de doble autenticación (2FA), en los equipos informáticos de gestión y operación de la producción que restringen el acceso a personal no autorizado?
5	¿Los empleados, incluido el personal de planta y de producción, reciben capacitación regular y periódica sobre buenas prácticas de seguridad informática?
6	¿La empresa tiene un sistema de respaldo (copias de seguridad o Backups), ya sea físico o en la nube, de su información crítica, en especial la de su cadena de producción?
7	¿La empresa evalúa y analiza de manera formal, regular y periódica , el nivel de riesgo cibernético asociado con la seguridad informática de sus equipos, sistemas y dispositivos informáticos, en especial de aquellos que están asociados a la gestión y operación de los procesos de producción?
8	¿Existe en su empresa un compromiso directivo y de la alta gerencia con respecto a la seguridad informática y la ciberseguridad de la organización?
9	¿Su empresa cuenta con maquinaria o equipos de su línea de producción que tengan conexión eventual, temporal o permanente a internet o a otras redes , ya sean internas (LAN – Red corporativa, como la del área de calidad, mantenimiento, etc.) o externas (proveedores, fabricantes, clientes, etc.)?
10	¿Ha sufrido su empresa incidentes o ataques informáticos en el pasado?
11	Utiliza un equipo computacional viejo y obsoleto en su cadena de producción?
12	¿Qué sistema operativo utiliza(n) su(s) equipo(s) computacional(es) asociados a la gestión de su cadena de producción?

PREGUNTA NRO.	OPCIÓN DE RESPUESTA (Escala de Likert)					
	0	1	2	3	4	5
1	18	3	1	0	2	4
2	1	4	10	3	2	5
3	6	6	5	1	4	3
4	2	2	13	0	2	6
5	18	5	0	2	1	2
6	0	1	6	4	6	8
7	8	5	4	0	5	2
8	2	7	7	1	2	6
9	3	8	5	0	4	5
10	4	0	0	0	0	21
11	3	3	7	2	7	3
12	Sistemas operativos identificados					
	Win XP	0		Win 11	17	
	Win 7	11		Linux	0	
	Win8	0		MacOS	0	
	Win 10	18				

Resultados fase 1 – Diagrama de barras verticales de hallazgos



Resultados fase 1 – Diagrama de Pareto



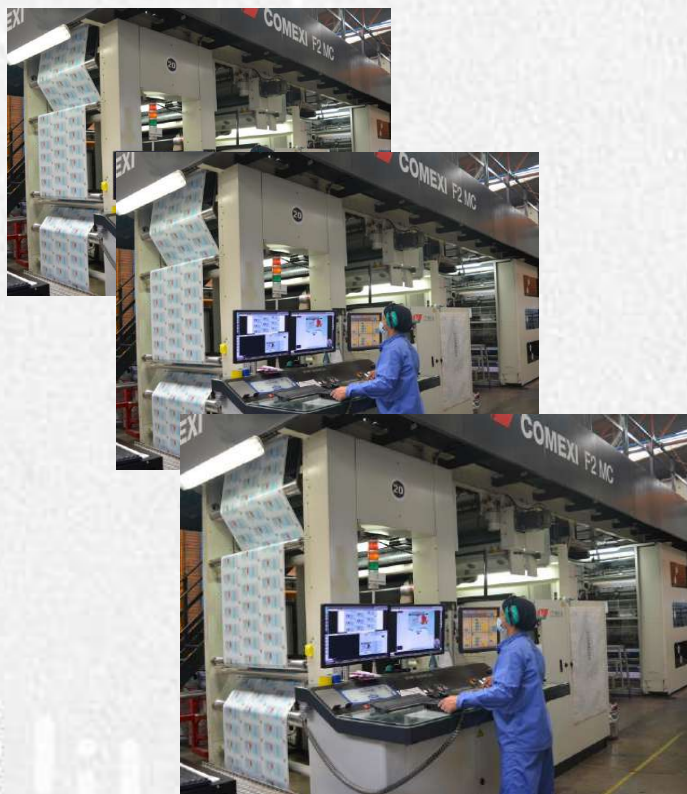
Resultados fase 1 - Matriz de Riesgo y Mapa de Calor

RIESGO	DESCRIPCIÓN DEL RIESGO
R1	Infección de equipos, cifrado de datos, pérdida de productividad e información.
R2	Secuestro o corrupción de datos críticos, No disponibilidad, manipulación de la información.
R3	Robo de datos confidenciales o sensibles, pérdida del respaldo físico y pérdida de la información.
R4	Caída de la red, interrupción del negocio, propagación de malware, interceptación de tráfico.
R5	Fallos de seguridad por falta de soporte, explotación del malware, interrupción de operaciones.
R6	Exposición a ataques dirigidos, robo credenciales, Malware / Ransomware.
R7	Escalada de privilegios, fuga de datos, ataques del día cero.
R8	Error humano, mal uso del sistema, alteración o manipulación.
R9	Exposición de red o sistemas internos, fuga de información, manipulación indebida.
R10	Sabotaje, Configuraciones incorrectas o exposición de datos.
R11	Riesgo de manipulación o pérdida de control interno, fuga información.
R12	Pérdida de información sensible como formulaciones, condiciones de máquina y otras especificaciones.
R13	Interrupción de producción por pérdida de datos críticos.

RIESGO	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD (1-5)	IMPACTO 1-16	GRAVEDAD DEL RIESGO (Probabilidad x Impacto)
R1	Infección de equipos, cifrado de datos, pérdida de productividad e información.	4	4	16
R2	Secuestro o corrupción de datos críticos, No disponibilidad, manipulación de la información.	4	16	64
R3	Robo de datos confidenciales o sensibles, pérdida del respaldo físico y pérdida de la información.	3	16	48
R4	Caída de la red, interrupción del negocio, propagación de malware, interceptación de tráfico.	3	8	24
R5	Fallos de seguridad por falta de soporte, explotación del malware, interrupción de operaciones.	4	4	16
R6	Exposición a ataques dirigidos, robo credenciales, Malware / Ransomware.	4	8	32
R7	Escalada de privilegios, fuga de datos, ataques del día cero.	4	4	16
R8	Error humano, mal uso del sistema, alteración o manipulación.	3	16	48
R9	Exposición de red o sistemas internos, fuga de información, manipulación indebida.	5	8	40
R10	Sabotaje, Configuraciones incorrectas o exposición de datos.	3	16	48
R11	Riesgo de manipulación o pérdida de control interno, fuga información.	3	16	48
R12	Pérdida de información sensible como formulaciones, condiciones de máquina y otras especificaciones.	4	16	64
R13	Interrupción de producción por pérdida de datos críticos.	4	16	64

Resultados fase 1 - Matriz de Riesgo y Mapa de Calor

Se constató la existencia de una brecha de seguridad en la industria flexográfica (nivel de madurez muy bajo en ciberseguridad), que se ve reflejada en la ausencia de procesos formales de gestión del riesgo, en la baja capacitación del personal, en la limitada gestión de activos digitales críticos y en la carencia de controles robustos de protección de la infraestructura TI asociada a la gestión, operación y control de la cadena de producción, lo cual configura un escenario preocupante de vulnerabilidad.



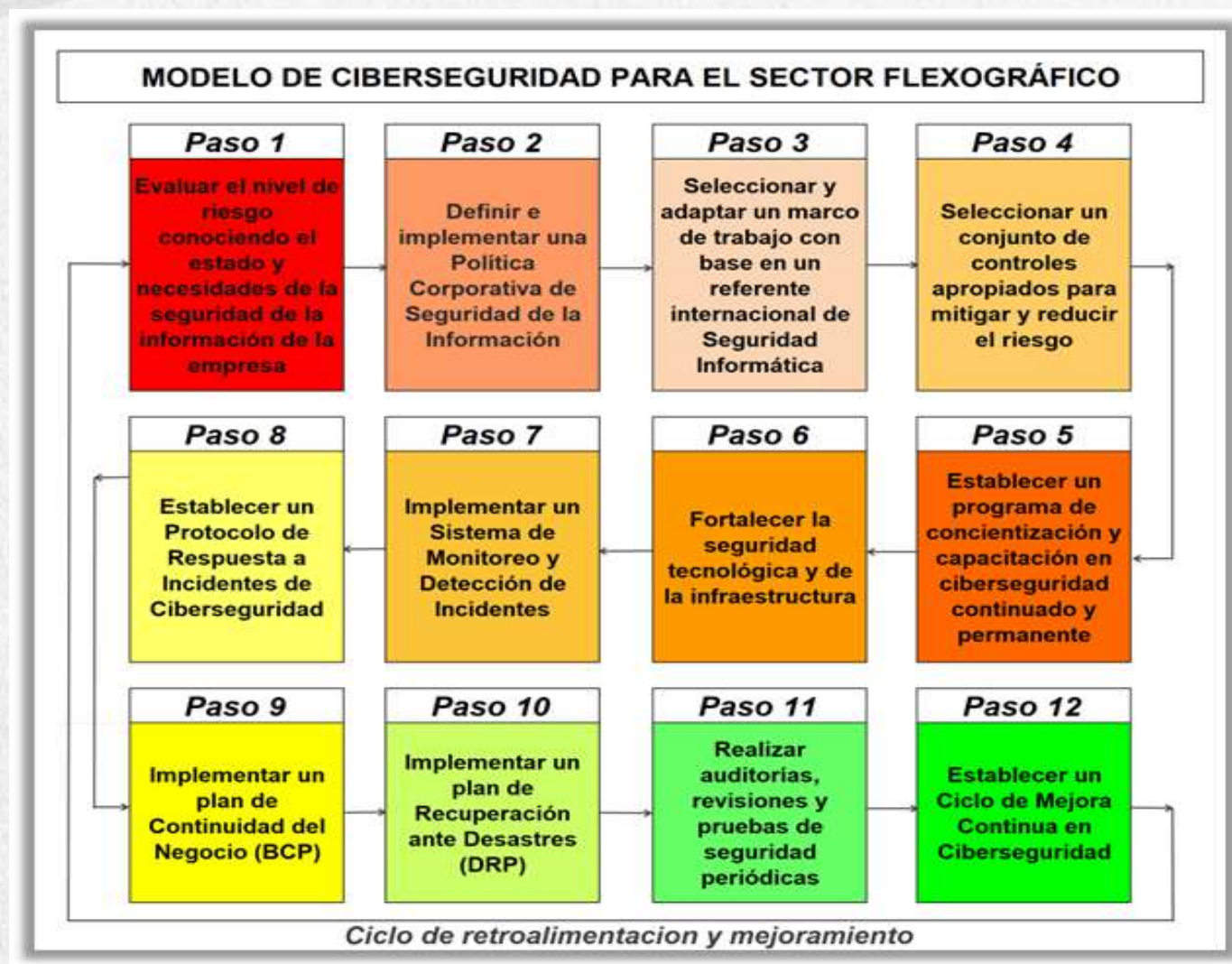
Resultados fase 2 - Análisis y revisión de estándares



**Resultado:
Selección de
controles y
consolidación del
diseño del modelo
de ciberseguridad**

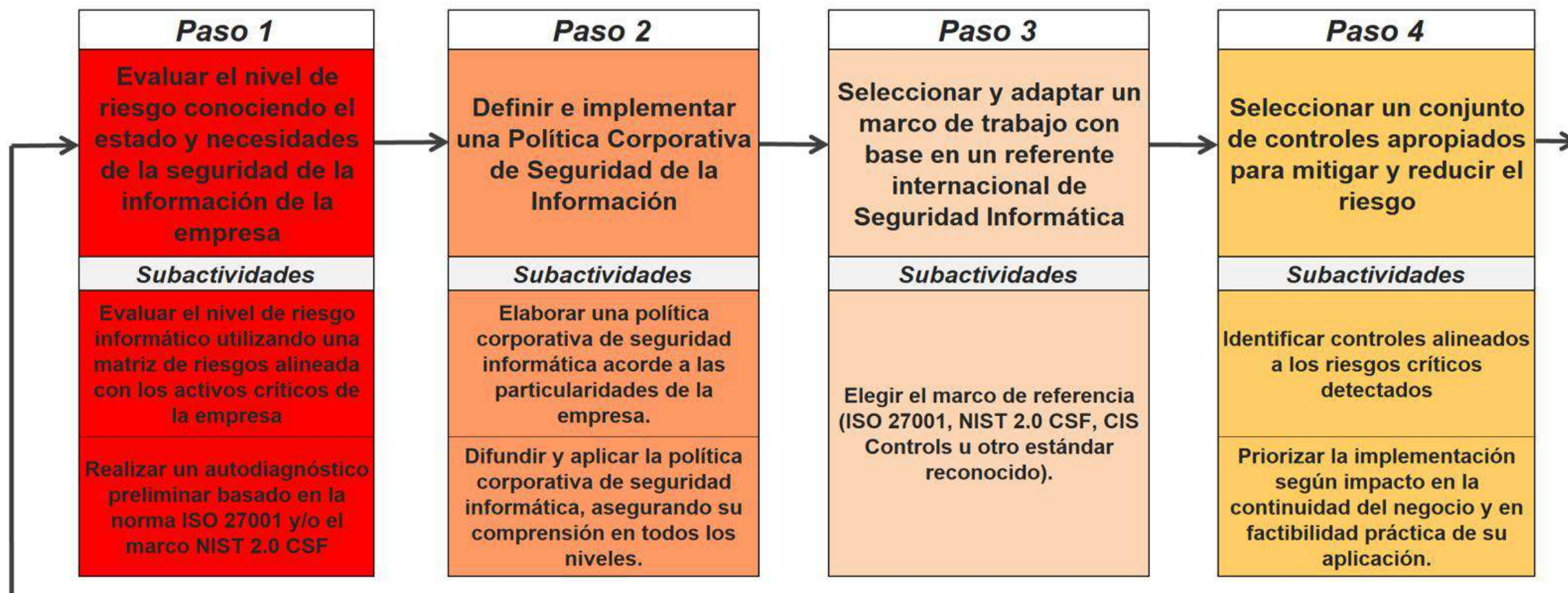


Resultados fase 2 – Modelo de ciberseguridad

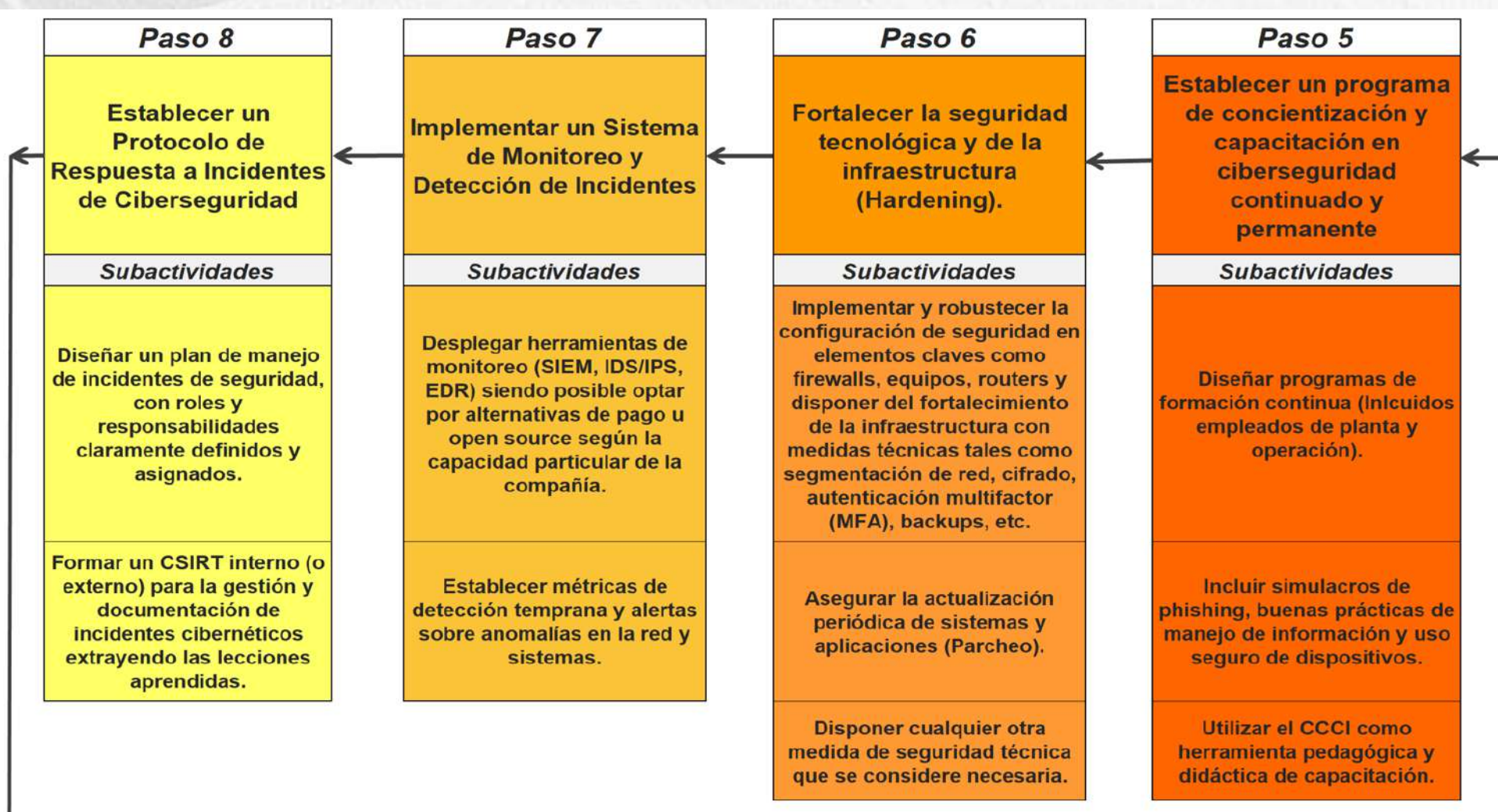


Fase 2: Detalle del modelo de ciberseguridad – subactividades (1/3)

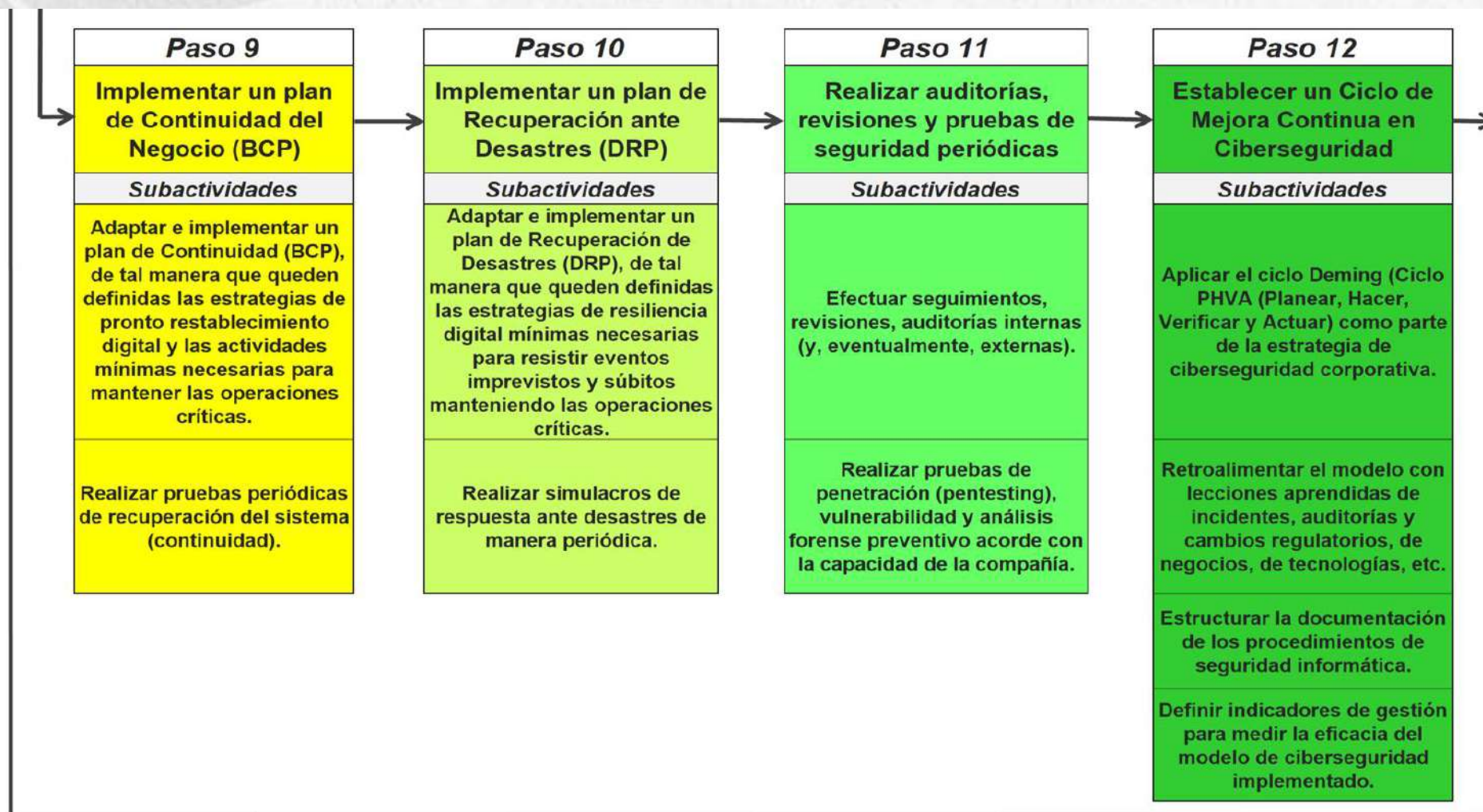
DESGLOSE DE LAS SUBACTIVIDADES DEL MODELO DE CIBERSEGURIDAD PARA EL SECTOR FLEXOGRÁFICO



Fase 2: Detalle del modelo de ciberseguridad – Sub actividades (2/3)



Fase 2: Detalle del modelo de ciberseguridad – subactividades (3/3)



Ciclo de retroalimentación y mejoramiento

Riesgos mitigados por cada uno de los pasos del modelo de ciberseguridad

Paso del Modelo de Ciberseguridad	Riesgos que mitiga	Explicación de la mitigación	Riesgo	Descripción del Riesgo
Paso 1: Evaluar el nivel de riesgo conociendo el estado y necesidades de la seguridad...	R9, R10	Al realizar un autodiagnóstico basado en NIST 2.0 CSF, se identifica la exposición de red y configuraciones incorrectas antes de que sean explotadas.	R1	Infección de equipos, cifrado de datos y pérdida de productividad.
Paso 2: Definir e implementar una Política Corporativa de Seguridad de la Información.	R11	Ataca directamente la pérdida de control interno y fuga de información mediante reglas claras para todos los niveles.	R2	Secuestro o corrupción de datos críticos y manipulación.
Paso 3: Seleccionar y adaptar un marco de trabajo con base en un referente internacional...	R3, R11	Mitiga el robo de datos y pérdida de control al usar estándares como ISO 27001, que obligan a proteger activos críticos.	R3	Robo de datos confidenciales y pérdida de respaldo físico.
Paso 4: Seleccionar un conjunto de controles apropiados para mitigar y reducir el riesgo.	R12	Permite priorizar la protección de "formulaciones y condiciones de máquina" al identificar controles alineados a riesgos críticos.	R4	Caída de la red, interrupción del negocio y malware.
Paso 5: Establecer un programa de concientización y capacitación en ciberseguridad...	R8	Es la defensa principal contra el "Error humano, mal uso del sistema, alteración o manipulación".	R5	Fallos por falta de soporte y explotación de malware.
Paso 6: Fortalecer la seguridad tecnológica y de la infraestructura (Hardening).	R1, R4, R5, R6	Al usar firewalls, MFA y parches, evita la infección de equipos, caídas de red y fallos por falta de soporte.	R6	Ataques dirigidos, robo de credenciales, malware y ransomware.
Paso 7: Implementar un Sistema de Monitoreo y Detección de Incidentes.	R6, R7, R9	Detecta ataques dirigidos, escalada de privilegios y fugas de información mediante herramientas como SIEM o EDR.	R7	Escalada de privilegios y ataques del día cero.
Paso 8: Establecer un Protocolo de Respuesta a Incidentes de Ciberseguridad.	R2, R13	Reduce el impacto del secuestro de datos al tener un equipo (CSIRT) que sabe cómo actuar ante la crisis.	R8	Error humano, mal uso del sistema o manipulación.
Paso 9: Implementar un plan de Continuidad del Negocio (BCP).	R4, R13	Mitiga la interrupción del negocio asegurando que existan estrategias para el pronto restablecimiento digital.	R9	Exposición de red o sistemas internos y fuga de información.
Paso 10: Implementar un plan de Recuperación ante Desastres (DRP).	R1, R2, R13	Ataca el cifrado de datos y pérdida de productividad mediante simulacros y restauración de sistemas.	R10	Sabotaje, configuraciones incorrectas o exposición de datos.
Paso 11: Realizar auditorías, revisiones y pruebas de seguridad periódicas.	R5, R7, R10	Identifica ataques de día cero y configuraciones incorrectas mediante pentesting y auditorías externas.	R11	Pérdida de control interno y fuga de información.
Paso 12: Establecer un Ciclo de Mejora Continua en Ciberseguridad.	Todos (R1-R13)	Evita que el modelo quede obsoleto, retroalimentándolo con lecciones aprendidas de incidentes reales.	R12	Pérdida de fórmulas, condiciones de máquina y especificaciones.
			R13	Interrupción de producción por pérdida de datos críticos.

Resultados fase 3 - Verificación del modelo de ciberseguridad mediante prueba conceptual

Actividad:

Se efectuó la aplicación de un instrumento metodológico (encuesta final).

Producto:

Los resultados obtenidos en la encuesta permitieron establecer la validez del prototipo cibernético protectivo. Adicionalmente, se logró constatar reducción del nivel de riesgo informático.

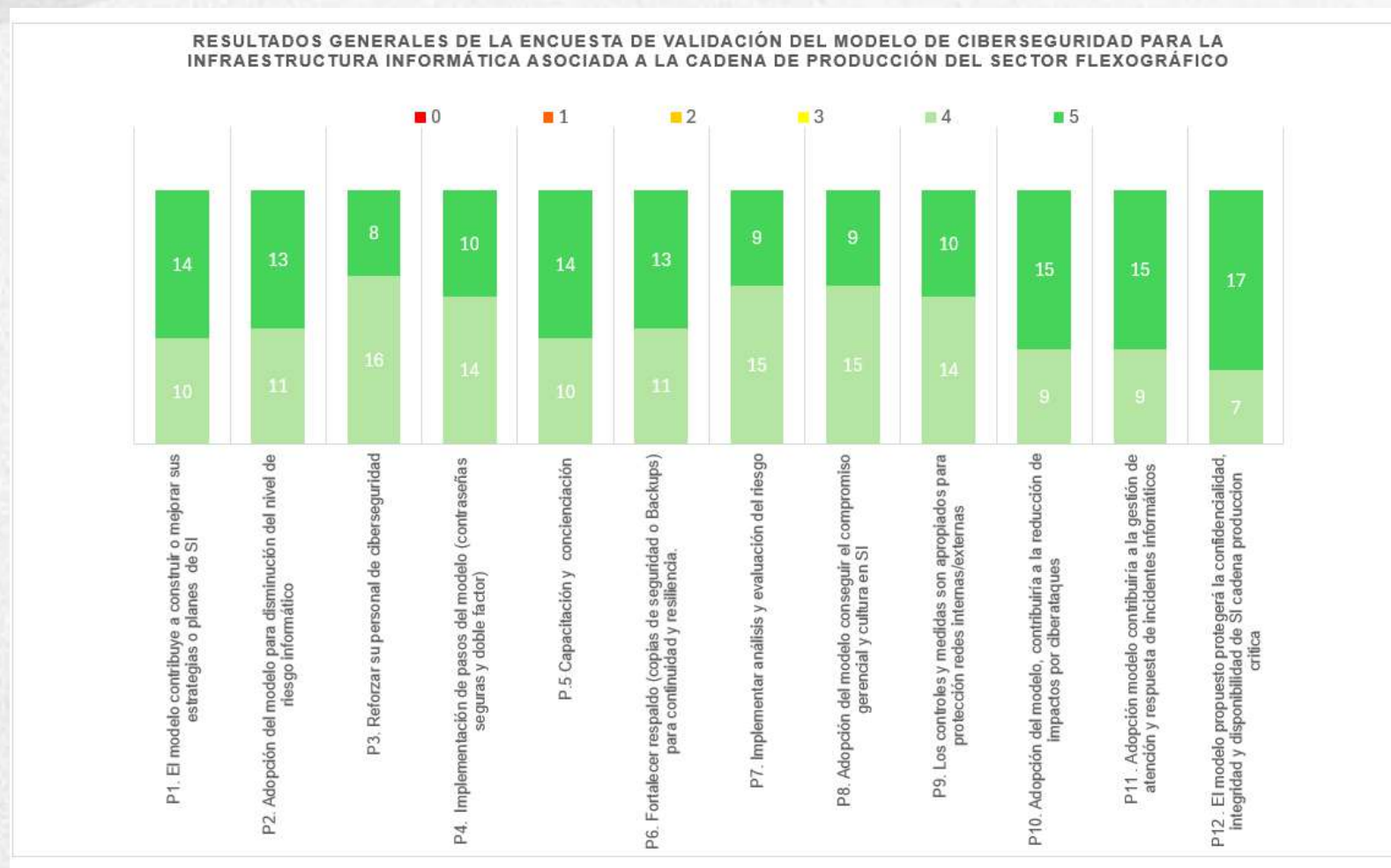


Resultados fase 3 – Hallazgos de la encuesta final de verificación del modelo

PREGUNTA NRO.	CUESTIONAMIENTO / PREGUNTA
1	¿En qué nivel cree Ud. que el modelo contribuye a construir o mejorar sus estrategias o planes de seguridad informática y, en general, a mejorar la ciberseguridad?
2	Considerando, en particular, las recomendaciones sobre cómo implementar medidas y controles de seguridad ¿En qué nivel cree Ud. que su adopción contribuiría a la disminución del nivel de riesgo informático?
3	¿En qué nivel consideraría Ud. que, reforzar su personal de ciberseguridad, ayudaría a mitigar y reducir su nivel de riesgo ante ciberataques e incidentes informáticos?
4	¿En qué nivel implementaría Ud. los pasos que se recomiendan y que se sugieren, entre ellos mejorar los controles de acceso con contraseñas más seguras y el uso de doble factor de autenticación, incluyendo implementar los controles respectivos sugeridos, para mejorar la protección y disminuir el riesgo cibernético?
5	¿En qué nivel consideraría Ud. implementar programas permanentes y continuos de capacitación y actualización en ciberseguridad para todo su personal?
6	¿En qué nivel cree Ud. que fortalecer su sistema de respaldo y recuperación de información de producción (production backup), incluida copia en la nube, sería conveniente, para garantizar la continuidad operativa y la resiliencia de su cadena de producción crítica?
7	¿En qué nivel considera Ud. que, implementar, de manera periódica, el análisis y evaluación del riesgo informático, con el fin de mitigar riesgos, sería una práctica de seguridad conveniente y recomendable para su empresa?
8	¿En qué nivel considera Ud. que su adopción contribuiría a conseguir, o fomentar, el compromiso de la gerencia con la ciberseguridad y a crear, o fortalecer, una cultura de seguridad informática al interior de su organización?
9	¿En qué nivel considera Ud. que los controles y medidas sugeridos son apropiados para la protección sus redes internas/externas y el aseguramiento de su conexión a internet?
10	¿En qué nivel considera Ud. que su adopción e implementación, contribuiría a la reducción o disminución de impactos negativos ocasionados por ciberataques?
11	¿En qué nivel considera Ud. que su adopción e implementación, contribuiría al mejoramiento de la gestión de atención y respuesta de incidentes informáticos?
12	En general, ¿En qué nivel considera Ud. que el modelo de ciberseguridad propuesto protegerá la confidencialidad, integridad y disponibilidad de la seguridad de la información de su cadena de producción crítica?

PREGUNTA NRO.	OPCIÓN DE RESPUESTA (Escala de Likert)					
	0	1	2	3	4	5
1					10	14
2					11	13
3					16	8
4					14	10
5					10	14
6					11	13
7					15	9
8					15	9
9					14	10
10					9	15
11					9	15
12					7	15

Resultados fase 3- Diagrama vertical de hallazgos de encuesta de verificación



Comparativo de la mitigación de riesgos lograda

Inicialmente diagnosticado

Mapa de aceptabilidad Inicial			
		% Distribución	Total Riesgos
Inaceptable	33 a 80	61.5	8
Tolerable	17 a 32	15.4	2
Aceptable	9 a 16	23.1	3
Muy Aceptable	3 a 8	0.0	0
Admisible	1 a 2	0.0	0
		100.0	13



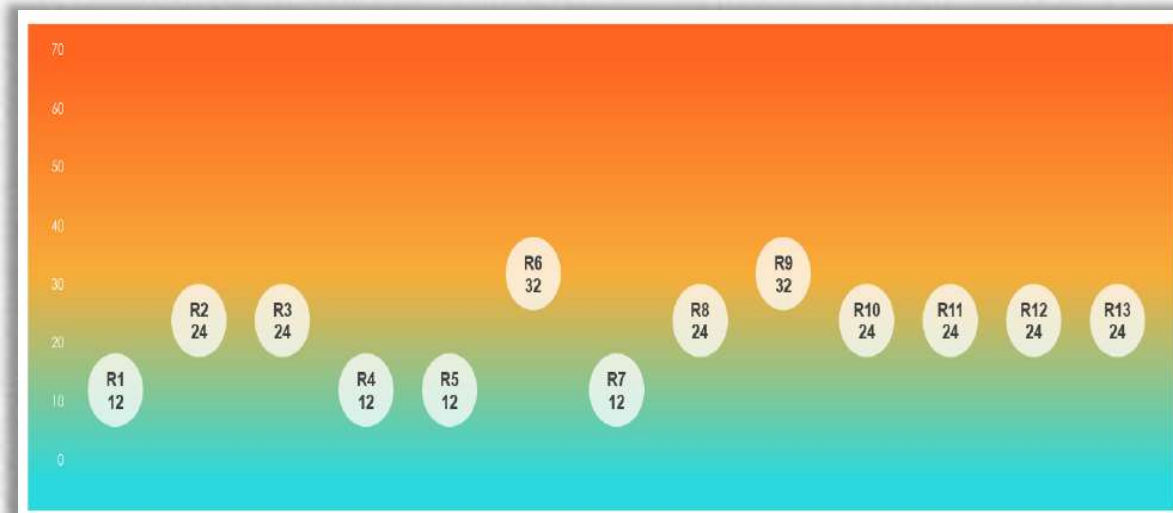
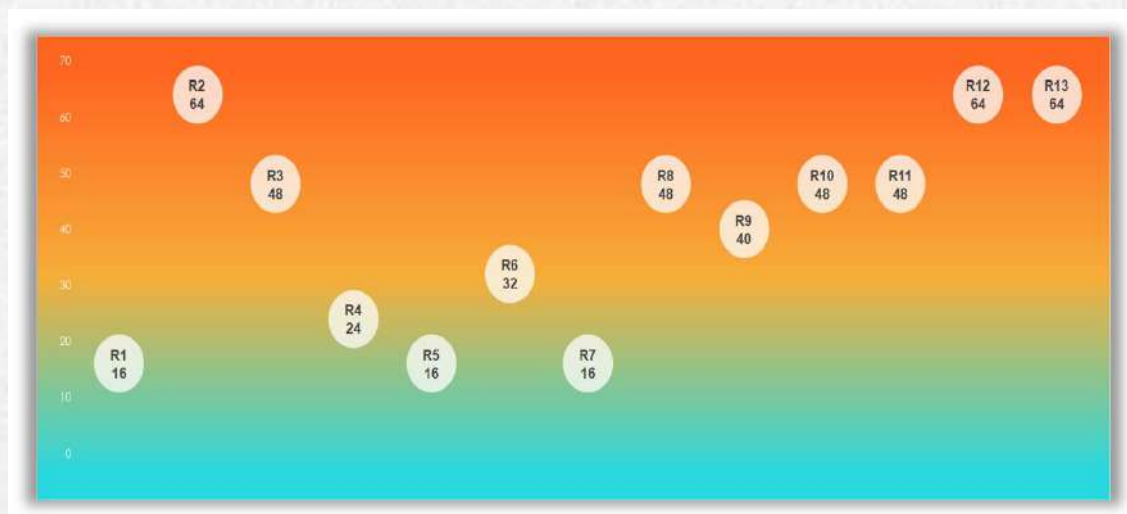
Mejorada con el modelo de ciberseguridad

Mapa de aceptabilidad x Validando el Modelo			
		% Distribución	Total Riesgos
Inaceptable	33 a 80	0.0	0
Tolerable	17 a 32	69.2	9
Aceptable	9 a 16	30.8	4
Muy Aceptable	3 a 8	0.0	0
Admisible	1 a 2	0.0	0
		100.0	13

Mapa de calor obtenido con el modelo de ciberseguridad

Inicialmente diagnosticado

Mitigado con el modelo de ciberseguridad





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años



El análisis comparativo entre el diagnóstico inicial y el estado final de la SI en la infraestructura TI, una vez socializado el modelo de ciberseguridad entre las compañías encuestadas de la industria flexográfica, muestra una mejora significativa y sustancial en la capacidad sectorial para gestionar la ciberdefensa.

Una vez que, en un trabajo futuro, se complete el modelo cibernético protectivo propuesto, incluyendo los sistemas OT, esta reducción será aun mayor, puesto que este trabajo solo protege la infraestructura TI.



CUBO CAMPANITO DE LA CIBERSEGURIDAD INDUSTRIAL (CCCI)

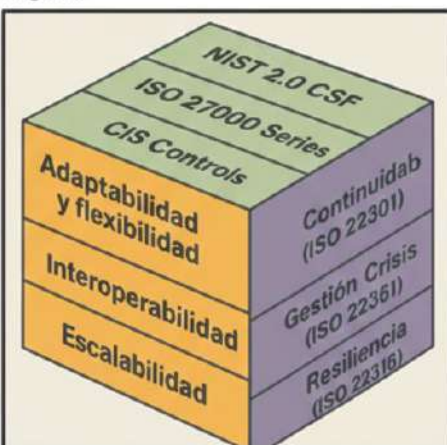
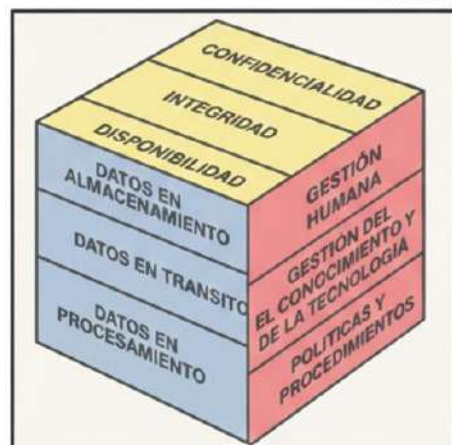
Cubo MacCumber (Original)

Extensión Dimensionales

Nivel Dimensional



Nivel de Categorías



Vista tridimensional general de la estructura conceptual (Niveles Dimensionales y Categorías).

Resultados de investigación complementarios

Nuevo marco CCCI

Industrial Cybersecurity Tinker Bell Cube (ICTBC framework)

El marco CCCI es una herramienta técnica de naturaleza pedagógica y didáctica que permite facilitar el proceso de comprensión, entendimiento y asimilación de los conceptos de ciberseguridad a personal no especializado.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

7

Conclusiones y recomendaciones





Conclusiones y Recomendaciones (1/3)

El sector flexográfico es una industria esencial, sin posibilidad de sustitución o remplazo en el corto plazo, que afecta, significativamente, a la economía, a la sociedad y a la vida de las personas, por lo cual, es tan necesario como urgente, fortalecer su ciberdefensa.

Las PYMEs del sector requieren de implementar, o fortalecer, su estrategia de ciberseguridad de manera práctica, efectiva y económica, de manera ajustada a su realidad, recursos y entorno.





Conclusiones y Recomendaciones (2/3)

Aun en organizaciones con recursos limitados y con una madurez cibernética inicial muy baja, como el caso de PYMEs, es posible establecer un modelo de ciberseguridad que, fundamentado en referentes y estándares internacionales y buenas prácticas de seguridad informática, de tal manera que, contribuyan al mejoramiento de la protección de la seguridad de la información, de forma progresiva, flexible, paulatina, adaptable y personalizable, acorde con las condiciones particulares de cada empresa.



Un hallazgo destacado es la disonancia entre la percepción de riesgo de los responsables de la ciberseguridad de las infraestructuras TI y la implementación efectiva de controles técnicos y administrativos que, ahora, el modelo de ciberseguridad propuesto, entra a solventar, mientras se realiza su complementación incluyendo los sistemas OT.

Es de resaltar que una parte significativa de los encuestados manifiesta reconocer la importancia de la ciberseguridad, pero, los datos obtenidos en los resultados demuestran que la adopción de medidas concretas sigue siendo parcial o inexistente.



Conclusiones y Recomendaciones (5/5)

Como demuestra la investigación realizada, la protección completa de la confidencialidad, integridad y disponibilidad de la SI en la industria flexográfica no se logra mediante la simple acumulación de herramientas tecnológicas, sino a través de la implementación de un modelo de gestión adaptativo que, incluyendo el modelo de ciberseguridad aquí propuesto, cierre la brecha entre el entorno IT (Oficina) y el OT (Planta), razón por la cual, este esfuerzo debe ser completado con un trabajo futuro enfocado en la protección de la infraestructura OT de la industria flexográfica.



CUBO CAMPANITO DE LA CIBERSEGURIDAD INDUSTRIAL (CCCI)

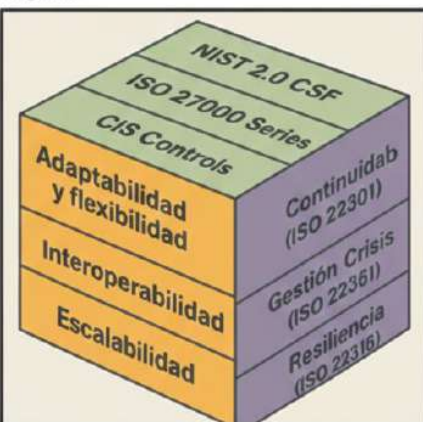
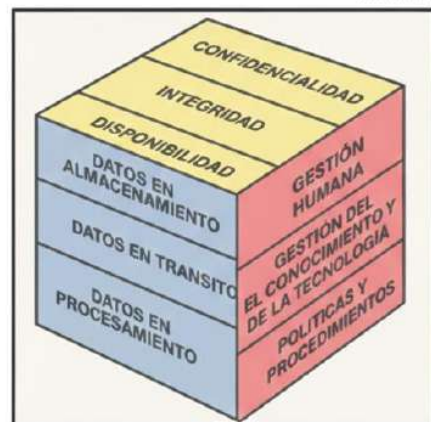
Cubo MacCumber (Original)

Extensión Dimensionales

Nivel Dimensional



Nivel de Categorías



Vista tridimensional general de la estructura conceptual (Niveles Dimensionales y Categorías).

Conclusiones y Recomendaciones (3/3)

Se logró la consolidación de un innovador marco de ciberseguridad basado en el nuevo CCCI (*ICTBC framework*), el cual es una extensión, actualización y mejora del cubo de McCumber de la seguridad informática.

Entre otras bondades, el CCCI articula de manera armónica las tradicionales dimensiones de McCumber, con el rigor de los estándares internacionales, las buenas prácticas de ciberdefensa y las necesidades actuales de los sectores industriales en cuanto a protección cibernética.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

8

Trabajos Futuros





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años



Trabajos Futuros (1/4)

Diseño de un modelo de ciberseguridad para la infraestructura OT asociada a la cadena de producción crítica de la industria flexográfica

Deberá incluir los sistemas OT que conforman la cadena de producción de la industria flexográfica





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años



Trabajos Futuros (2/4)

Prototipo de ciberseguridad industrial avanzado potenciado con herramientas de inteligencia artificial (IA)

Evaluación del nivel de madurez en ciberseguridad de las PYMEs del sector flexográfico bajo los referentes NIST 2.0 CSF e ISO 27000 series.





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años

Trabajos Futuros (3/4)

Diseño de indicadores de desempeño en ciberseguridad para la infraestructura TI de la industria flexográfica basados en buenas prácticas internacionales.

Análisis comparativo de modelos de ciberseguridad aplicados a cadenas productivas industriales: caso del sector flexográfico vs. otros sectores.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

Trabajos Futuros (4/4)



Tesis Doctoral

Potenciación de un modelo de ciberseguridad por medio de inteligencia artificial para la cadena de producción crítica de la industria flexográfica y convertidora.

Incluye: sector convertidor y de transformación de plásticos, infraestructura y sistemas OT y el diseño e implementación de una herramienta basada en inteligencia artificial.

Actualmente, este proyecto forma parte de las línea de investigación en CTS del nuevo Doctorado en Ciencia y Tecnología de ITM y Pascual Bravo.



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

9

Productos





Institución
Universitaria | 80
Reacreditada en Alta Calidad | Años

A. Publicaciones:

1) Revista La Tekné de ITM, 118(ed. 2025)

2) Springer Lectures Notes in Computer Science (Capitulo de Libro), Abril/26

<https://link.springer.com/book/9789819575794>

3) Revista de la U. Militar Nueva Granada, 2026

4) Cuadernos Activa Nro. 18 - Ene-Jun 2026





Institución
Universitaria | 80
Reacreditada en Alta Calidad | Años

B) Ponencias:

1) Simposio Nacional de Maestrías y Doctorados 2025 del 19 Congreso Colombiano de Computación de la Sociedad Colombiana de Computación SoC. - 8 Sept. / 2025 ;

2) LACLO Medellín 2025, P.C.J.I.C. / T.de.A, 6-7 nov. / 2025;

3) Seminario de Ciberdefensa, UNAULA; 6-mzo 2026;

4) Grupo de investigación en Inteligencia Computacional. P.C.J.I.C./ T.de.A., 10-mzo-26;





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años

C) Ponencias 2026 / 2027:

1) Simposio Nacional de Maestrías y Doctorados 2026 (SMYD26) del 20 Congreso Colombiano de Computación (20CCC) de la Sociedad Colombiana de Computación (SCo2). – Cartagena, 8 Sept. / 2026

2) Bootcamp Internacional de Ciberseguridad de la Asociación Internacional de Ciberseguridad – ASICI, 21 a 25 Oct. / 2026 ;

3) RSAC SF27 - Rivest, Shamir & Adleman Conference, San Francisco, CA, U.S.A., 5-8 Abril / 2027

SCo²

SOCIEDAD COLOMBIANA
DE COMPUTACIÓN

20 CONGRESO COLOMBIANO
DE COMPUTACION

ASICI

Asociación Internacional
de Ciberseguridad



Bootcamp Internacional de Ciberseguridad - ASICI
21, 22, 23, 24, 25 de octubre



EN DIRECTO
YouTube

RSAC 2027 Conference

RSAC | Conference

RSAC 2027 Conference
World's leading cybersecurity conference
Dates: Monday, April 5, 2027 - Thursday, April 8, 2027
Venue: Moscone Center, San Francisco CA, United States



CERTIFICADO DE MEMBRESÍA

El presente certificado reconoce que

ADRIANA MARÍA ECHEVERRI LONDOÑO

Es miembro activo de la Asociación Internacional de Ciberseguridad - ASICI, celebramos su compromiso con la integridad, la confianza y el desarrollo de buenas prácticas en ciberseguridad.

Este certificado acredita la membresía correspondiente al año 2026.

Madrid, España



Mauricio Fraydinet Delgado
Presidente

Código: 4134167755-4051-042-000000000000



CERTIFICADO DE MEMBRESÍA

El presente certificado reconoce que

EDGAR ALBERTO ACEVEDOARANGO

Es miembro activo de la Asociación Internacional de Ciberseguridad - ASICI, celebramos su compromiso con la integridad, la confianza y el desarrollo de buenas prácticas en ciberseguridad.

Este certificado acredita la membresía correspondiente al año 2026.

Madrid, España



Mauricio Fraydinet Delgado
Presidente

Código: 334642-040-4051-042-000000000000



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

10

Referencias



Referencias (1/3)

S. A. Berru Escajadillo, y L. F. Yarleque Golles. “Propuesta Metodológica para mitigar los Riesgos sobre Ciberataques a PYMEs, usando la metodología NIST”. TGP. Tesis de Pregrado. Ingeniería de Sistemas. Facultad de Ingeniería y Arquitectura. Universidad César Vallejo. Piura, Perú. 2023. Págs. 95.

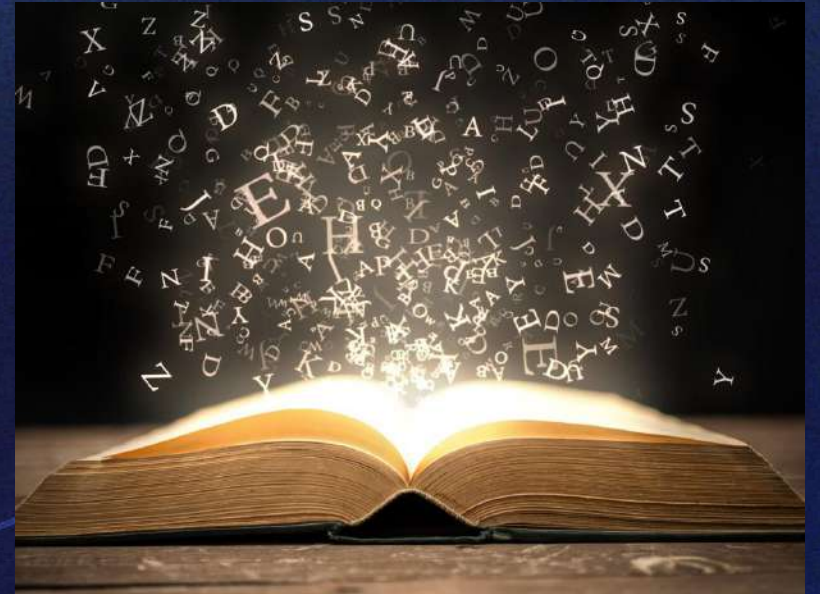
Disponible

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/128701/Berru_ESA-Yarleque_GLF-SD.pdf?sequence=1&isAllowed=y

en:

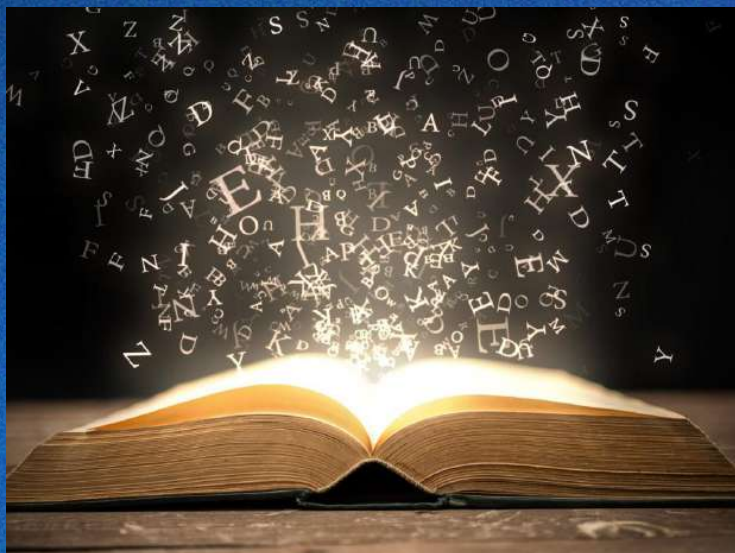
O. Bustillos Ortega, y J. Rojas Segura. “Protocolo Básico de Ciberseguridad para PYMEs”. Paper. Artículo de Revista Técnica. Revista INTER FASES. Nro. 16. ISSN 1993-4912. Diciembre de 2022. p.p. 166 – 184.

Disponible en: <https://revistas.ulima.edu.pe/index.php/Interfases/article/view/6021/6043>





Referencias (2/3)



J. M. Rodríguez López. "Defensa de Infraestructuras críticas: el rol de la inteligencia artificial en la ciberseguridad". Webminar On Line. Sociedad Colombiana de Computación – SCo2 – Capítulo CISI2, ITM, UNAD, U. del Cauca. U. Javeriana, U. de Antioquia y I.U. Colegio Mayor del Cauca. 30 de Octubre de 2024.

Disponible en: [Webinar Defensa de Infraestructuras Críticas El Rol de la Inteligencia Artificial en la Ciberseguridad-20241030 180546-Grabación de la reunión.mp4](#)

Y. Z. Giraldo Montes. "Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad". Tesis de Grado de Maestría. Maestría en Seguridad Informática, Instituto Tecnológico Metropolitano - ITM, Medellín, 2020.

Disponible en: <https://repositorio.itm.edu.co/handle/20.500.12622/5550>



Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

Referencias (3/3)

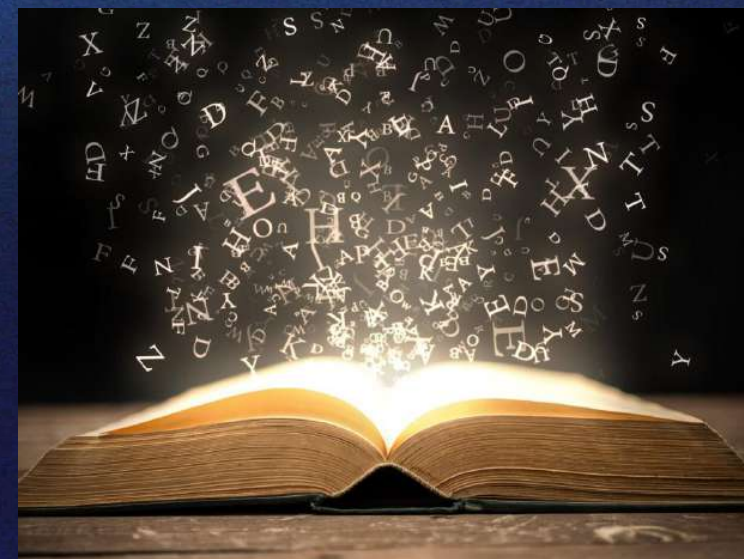
H. Valencia Valencia y F. H. Orjuela Gómez, "Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa". Tesis de Grado de Maestría. Maestría en Seguridad Informática. Facultad de Ingeniería. Instituto Tecnológico Metropolitano - ITM, Medellín, 2021.

Disponible en: <https://repositorio.itm.edu.co/handle/20.500.12622/5197>

R. D. Villa Trujillo. "Modelo de ciberseguridad en las unidades de medición fasorial (PMU) del nuevo sistema inteligente de supervisión y control avanzado de tiempo real (ISAAC) del sistema eléctrico nacional". Tesis de Investigación de Maestría en Seguridad Informática. Facultad de Ingenierías. Grupo de Investigación en Automática y Electrónica y Ciencias computacionales. I.T.M. Medellín, Ant., Colombia. 2019. pp. 94.

Disponible en:

<https://repositorio.itm.edu.co/handle/20.500.12622/5197>





Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

11

Agradecimientos





Institución
Universitaria
Reacreditada en Alta Calidad | 80 Años

Agradecimientos

Los autores agradecen A:

- **SERVIFLEX ARCO Internacional S. A. S.,**
- **I.T.M.,**
- ***Nuestros directores, a nuestros jurados, a nuestros docentes, a nuestros compañeros,***
- **Nuestras familias,**
- **Sector Flexográfico Colombiano,**
- **Todos aquellos que por brevedad se omiten, pero, que de una u otra forma colaboraron para la consolidación de esta investigación y de este camino de aprendizaje en la M.S.I. de I.T.M.**





Institución
Universitaria
Reacreditada en Alta Calidad

80
Años

!Muchas Gracias!



**THANK YOU
FOR YOUR
ATTENTION**