Institución Universitaria

Sistema de gestión de ciberseguridad industrial enfocado a las tecnologías de la operación para mitigar posibles riesgos en las plataformas industriales del sector manufactura-textil

Iván Darío Lopera Salcedo

Instituto Tecnológico Metropolitano

Maestría en Seguridad Informática

Medellín, Colombia

Octubre 2023

Sistema de gestión de ciberseguridad industrial enfocado a las tecnologías de la operación para mitigar posibles riesgos en las plataformas industriales del sector manufactura-textil

Iván Darío Lopera Salcedo

Trabajo de investigación presentado como requisito para optar al título de:

Magister en Seguridad Informática

Directores:

Leonardo Serna Guarín – MSc.

Miguel Alberto Becerra Botero – Ph.D

Instituto Tecnológico Metropolitano

Maestría en Seguridad Informática

Medellín, Colombia

Octubre 2023

Dedicatoria

Este proyecto de grado se lo dedico primero que todo a Dios, ser supremo que me dio la vida y me ha cuidado en cada uno de mis pasos; en segunda instancia, se lo dedico a mi familia, agradezco el entendimiento y el apoyo brindado durante mis años de estudio y en tercera instancia, se lo dedico a mis profesores, gracias por compartir su conocimiento y experiencia.

RESUMEN

Con el acelerado desarrollo tecnológico que experimenta la industria 4.0, cada día son más los dispositivos industriales del sector manufactura-textil que se conectan a las redes corporativas. Esta interconexión se orienta principalmente a la generación de métricas y la optimización de procesos, con el objetivo de aumentar la productividad. Estos dispositivos industriales forman parte de lo que hoy conocemos como tecnologías de la operación (TO), las cuales requieren un tratamiento y enfoque diferenciado en comparación con el convencionalmente aplicado en el ámbito de las tecnologías de la información (TI). Las características distintivas de los dispositivos que integran las tecnologías de la operación son múltiples, en primer lugar, suelen operar con sistemas operativos obsoletos o legados, lo que dificulta la aplicación de parches de seguridad y las actualizaciones. Además, la instalación de endpoints de seguridad suele ser inviable por la compatibilidad y por su naturaleza industrial, sus protocolos no son identificados por los firewalls convencionales que se utilizan en TI.

Por lo anterior, el ambiente de las TO conlleva una gran cantidad de vulnerabilidades que podrían ser aprovechadas o explotadas por amenazas tanto internas como externas. Esto plantea una preocupación significativa debido a que dichas amenazas podrían tener el potencial para causar un impacto sustancial en las organizaciones del sector manufactura textil donde hacen uso de estos dispositivos industriales, poniendo en riesgo activos críticos y la continuidad de las operaciones.

El presente proyecto propone un modelo de gestión de ciberseguridad industrial enfocado a las tecnologías de la operación que permita mitigar los riesgos de seguridad informática en las plataformas industriales del sector manufactura-textil. Para la construcción de este modelo, se realizó la caracterización a través de un análisis de relevancia de los principales marcos de referencia y posterior a su análisis, se identificaron los marcos de ciberseguridad más alineados para la presente investigación. Posteriormente, se realizó la construcción del sistema de gestión de ciberseguridad industrial enfocado en las TO donde se definieron los diferentes dominios que conforman el modelo. Por último, se llevó a cabo la validación del modelo de gestión de ciberseguridad industrial a través de un caso de estudio en una empresa del sector manufactura-textil, este enfoque práctico garantizó la aplicabilidad y la eficacia del modelo desarrollado en un entorno real.

Palabras clave: Revolución industrial, Tecnologías de la operación, Internet de las cosas, Ciberseguridad industrial, Sistema de gestión de ciberseguridad, Estándares de ciberseguridad industrial.

ABSTRACT

With the accelerated technological development experienced by the industry 4.0, every day, more industrial devices in the textile manufacturing sector are connecting to corporate networks. This interconnection is primarily aimed at generating metrics and optimizing processes with the goal of increasing productivity. These industrial devices are part of what we now know as Operational Technologies (OT), which require a differentiated treatment and approach compared to what is conventionally applied in the field of Information Technologies (IT). The distinctive features of the devices that make up Operational Technologies are manifold. Firstly, they often operate with outdated or legacy operating systems, which hinders the application of security patches and updates. In addition, the installation of security endpoints is often unfeasible due to compatibility issues, and, due to their industrial nature, their protocols are not identified by conventional firewalls used in IT.

As a result, the environment of Operational Technologies entails a multitude of vulnerabilities that could be exploited by both internal and external threats. This raises significant concerns since these threats have the potential to cause a substantial impact on organizations in the textile manufacturing sector where these industrial devices are used, putting critical assets and business continuity at risk.

The present project proposes a model of industrial cybersecurity management focused on Operational Technologies to mitigate the risks of cybersecurity in industrial platforms within the textile manufacturing sector. To construct this model, a characterization was performed through an analysis of the relevance of the main reference frameworks, and after the analysis, the most aligned cybersecurity frameworks for this research were identified. Subsequently, the construction of the industrial cybersecurity management system focused on Operational Technologies was carried out, defining the various domains that comprise the model. Finally, the validation of the industrial cybersecurity management model was carried out through a case study in a company in the textile manufacturing sector, ensuring the applicability and effectiveness of the model developed in a real-world environment.

Keywords: Industrial Revolution, Operation Technologies, Internet of Things, Industrial Cybersecurity, Cybersecurity Management System, Industrial Cybersecurity Standards.

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ABREVIATURAS

ACL: Listas de control de acceso

CIO: Director de sistemas de la información

CISO: Oficial de seguridad de la información

ETSI: Instituto Europeo de Estándares de Telecomunicaciones

IACS: Sistemas de control y automatización industrial

ICS: Sistemas de control industrial

IEC: Comisión electrotécnica internacional

IIoT: Internet de las cosas industrial

IoT: Internet de las cosas

ISA: Sociedad Internacional de Automatización

ISO: Organización Internacional de normalización

TI: Tecnologías de la Información

NIST: Instituto Nacional de Estándares y Tecnología

TO: Tecnologías de la Operación

PERA: Arquitectura de referencia corporativa Pardue

PLC: Controlador lógico programable

SCADA: Control, supervisión y adquisición de datos

SCADA: Supervisión, control y adquisición de datos

SGCI: Sistema de gestión de ciberseguridad industrial

TCP: Protocolo de control de transmisión

VLAN: Red de área local virtual

CCI: Centro de ciberseguridad industrial

INTRODUCCIÓN

Las tecnologías de la información y la comunicación (TIC's) y el ciberespacio desempeñan un papel fundamental en la globalización actual, este tipo de tecnologías habilitan a los diferentes sectores públicos, privados, medios de comunicación, fuerzas públicas, gobiernos y el tejido empresarial para desarrollar a cabalidad sus respectivas actividades. Sin embargo, la mayoría de los servicios esenciales y los propios activos de tecnología dependen cada vez más de las infraestructuras industriales las cuales juegan un papel importante en los avances tecnológicos [1]. Los sistemas de información y los sistemas de control industrial, se encuentran expuestos a un creciente número de amenazas y riesgos debido a que estos sistemas son propensos a incidentes de seguridad que pueden llegar a afectar los activos de información. Entre los posibles incidentes se encuentran fraudes, espionajes, sabotajes, robo de información o vandalismo. Estos incidentes pueden ser causados tanto de forma voluntaria como involuntaria por personal interno o externo a la organización, o incluso por catástrofes naturales de forma accidental [2].

La industria 4.0 o la revolución industrial se relaciona directamente con las plataformas de las tecnologías de la operación (TO), este tipo de tecnologías son impulsadas por la automatización al poder incorporar dispositivos de internet de las cosas que permiten digitalizar las cadenas de producción y de suministro creando redes de comunicación entre las máquinas, permitiendo la generación de millones de bits para posteriormente con ayuda de herramientas de software convertirlos en información confiable e interesante para las organizaciones, las cuales ayudan a aumentar la eficiencia en las industrias y reducir los costes de fabricación de los productos [3].

Las infraestructuras industriales son la base de las infraestructuras críticas y los servicios esenciales, es por esto que se han convertido en un objetivo para los actos de ciberterrorismo a nivel mundial. Adicionalmente, la ausencia de seguridad como requisito en el diseño, implantación y operación de este tipo de tecnologías, ha llamado la atención de los ciber-atacantes quienes están dispuestos a sacar provecho de un sin número de vulnerabilidades existentes en los entornos de las tecnologías de la operación; es claro que nuestra sociedad y economía es vulnerable, casos como los de Stuxnet, Anonymous, las Botnets o los ataques de denegación de servicios son términos cada vez utilizados y se refieren a fugas de información, pérdidas o suspensión de servicios, entre otras incidencias [1].

Debido a la convergencia de las tecnologías, la superficie de exposición de las TO ha aumentado debido a las capacidades débiles que tienen los dispositivos frente a la ciberseguridad y la carencia de actualizaciones de seguridad que minimicen las vulnerabilidades de los dispositivos [4]. A esto se le suma que los administradores de infraestructuras TO no tienen los riesgos identificados ni un plan de respuesta de incidentes contra los ataques industriales, adicionalmente, no tienen visibilidad completa sobre los activos de información ni la conciencia frente a la protección de las amenazas del entorno. Es por esto que diferentes organizaciones como la *International Society of Automation* (ISA), la *International Organization for Standardization* (ISO), el *National Institute of Standards and Technology* (NIST) y los gobiernos a nivel mundial están trabajando en marcos y estándares que ayudan a mitigar el impacto de los riesgos por el uso de las TO en las industrias [5].

Considerando lo anteriormente expuesto, se evidencia la pertinencia de “Proponer un modelo de gestión de ciberseguridad industrial enfocada a las tecnologías de la operación para mitigar los riesgos de seguridad informática en las plataformas industriales del sector manufactura-textil basado en las mejores prácticas de los marcos de ciberseguridad ISA/IEC, ISO, y NIST”. En este estudio se propone “Caracterizar los estándares y sistemas de gestión de ciberseguridad por medio de un análisis de relevancia de sus diferentes niveles que permita mitigar los riesgos de las TO en el sector manufactura-textil.” lo cual permitirá “Construir un sistema de gestión de ciberseguridad industrial enfocado en las TO del sector manufactura-textil soportado por las mejores prácticas de los marcos de ciberseguridad” para finalmente “Validar el sistema de gestión de ciberseguridad industrial enfocado en las TO a través de un caso de estudio en una empresa del sector manufactura-textil”.

MARCO TEÓRICO Y ESTADO DEL ARTE

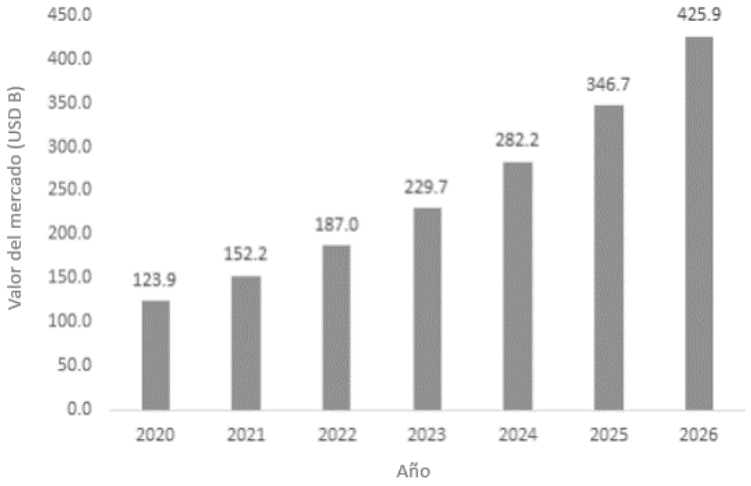
En el presente capítulo se abordan las tendencias, los conceptos, las investigaciones y los avances más relevantes de la ciberseguridad industrial orientados a las plataformas de las tecnologías de la operación; así mismo, se identificó cómo a través de los estándares globales de las tecnologías de la información se ha impactado en la mitigación de riesgos de los ambientes industriales, los cuales, anteriormente estaban aislados y no estaban conectados a las redes de comunicación. Gracias al auge de los equipos de IoT y a sus implementaciones, actualmente se menciona sobre la convergencia de estos ambientes, el TI y el TO. Adicionalmente, los riesgos que estaban presente en cada uno de estos ambientes ahora son compartidos y deben ser asegurados y gestionados por las organizaciones.

MARCO TEÓRICO

Las tendencias de mercado anticipan un incremento de dispositivos de IoT, los cuales están conectados a las redes y cuentan con diferentes sensores que permiten comunicarse con personas, con el ambiente y entre los mismos dispositivos, por esto, en lo que lleva del año se ha tenido un crecimiento global de 7.2 billones de dispositivos electrónicos conectados a las redes [6]. Las plataformas TO, son objeto de robo de información y de actos perjudiciales en servicios críticos por no tener consolidado un mapa que los oriente a proteger la infraestructura de IoT y que permita asegurar los pilares de la seguridad informática [5]. La industria de tecnología indica que las TO permiten que las fábricas funcionen y que gracias a los avances de este tipo de tecnología, se han generado mejoras respecto a la eficiencia operativa en la economía, debido a esto, las ventas anuales de hardware y software de TO han alcanzado los 40 mil millones de dólares para el presente año después de crecer más del 6% anual durante los últimos cinco años donde se ha identificado que el mayor gasto está relacionado con la convergencia de los ambientes; estas integraciones, permiten aumentar la eficiencia operativa y la rentabilidad de las empresas, ahora, lo que inicialmente estaba desconectado de la red actualmente dependen de conexiones con los sistemas TI conectados incluso con sitios en internet, esto implica un mayor riesgo de seguridad para los sistemas industriales debido a que la superficie de ataque aumenta considerablemente [7].

El tamaño del mercado del IIoT se valoró en US $ 123,89 mil millones en 2020, y se estima que crecerá alrededor de 22,85% CAGR durante 2021-2026 como se puede apreciar en la *Figura 1*. Por otro lado, se destaca el aumento de la penetración de las fábricas inteligentes, los servicios públicos inteligentes que permiten la transmisión de datos de alta velocidad y el análisis de datos para el control y la supervisión en tiempo real para impulsar el mercado de Internet de las cosas. La creciente demanda de computación avanzada y las tecnologías relacionadas de la era digital, como la inteligencia artificial, el aprendizaje automático para la automatización industrial que permite la convergencia de TI y TO contribuye al crecimiento del mercado, esto también gracias a la digitalización de los procesos operativos y el sistema de control industrial incluyendo interfaces hombre-máquina, sistemas de control de supervisión y adquisición de datos, sistemas de control distribuido y controladores lógicos programables que permiten optimizar los procesos, aprovechando la incorporación de sensores inteligentes, el acceso y los controles remotos, los cuales contribuyen al crecimiento del mercado [8].

Figura 1. Valor del mercado del IoT industrial global.



Nota. Mercado global del IoT industrial 2020-2026 Fuente: Adaptado de [8].

En el entorno industrial, se presentaba una falsa sensación de seguridad basada principalmente en cinco ideas preconcebidas: la planta está aislada (no está conectada a internet), se tiene un firewall que protege a la organización, los hackers no saben de sistemas/procesos industriales, la planta no es objetivo de nadie y los sistemas de seguridad de planta protegen la infraestructura de los ciberataques, sin embargo, el riesgo que se debe gestionar está asociado a la probabilidad de que los activos sufran una indisponibilidad o pérdida de integridad para prestar el servicio; adicionalmente, impacta la visibilidad o superficie de exposición, que en las redes de entornos industriales TO se ha visto incrementada en los últimos años, por lo tanto, aumenta la probabilidad de un incidente de ciberseguridad [9].

Por tal razón, TO es un objetivo por los ciberdelincuentes. Los productores de tecnología mencionan que los dispositivos y redes TO no se diseñaron teniendo en cuenta la seguridad, estos equipos normalmente estaban protegidos por lo que se denomina un “air gap”, lo que significa que estaban físicamente aislados y no conectados de alguna manera a las redes TI e Internet, pero una vez que TO se conecta al mundo, está expuesto a nuevos riesgos y los ataques cibernéticos en TO pueden causar problemas mucho mayores como por ejemplo tomar control de una línea de producción de manera remota [4].

Los sistemas de infraestructura crítica que requieren un mayor tiempo de actividad para mantener la calidad de vida también son convergentes y las iniciativas de TO impulsadas por las diferentes compañías exponen activos operativos altamente críticos a riesgos potenciales e infracciones de seguridad en las cuales los sistemas TO controlan estas infraestructuras críticas [4]. En reconocimiento de este peligro, se emitió la directiva de política presidencial 21 (PPD-21): Seguridad y resiliencia de infraestructura crítica. El objetivo de esta norma es fortalecer y asegurar la infraestructura crítica en los EE.UU reduciendo las vulnerabilidades, deteniendo las amenazas y minimizando consecuencias de los ataques a infraestructuras críticas; la directiva señala que es una responsabilidad compartida entre las autoridades federales, estatales, locales, entidades territoriales, propietarios y operadores públicos y privados de infraestructura crítica [10]. La norma detalla los diferentes sectores de infraestructura crítica los cuales son descritos en la Tabla 1. Los

ataques a la fabricación o a los ambientes industriales pueden no parecer críticos, pero si un ciberdelincuente decide manipular equipos en fábricas que producen alimentos, estos podrían ser inseguros y podrían distribuirse y venderse sin pasar por los controles de seguridad y calidad correspondientes; si un hacker modifica la composición de una semilla producida para cultivar alimentos, los cultivos que de allí se deriven fallan, lo que podría resultar en una escasez de alimentos [4].

Tabla 1. Sectores de infraestructura crítica en la política presidencial 21 EE.UU

Químico	Represas	Servicios financieros	Tecnologías de la información
Instalaciones comerciales	Defensa de base industrial	Comida y agricultura	Reactores, materiales y desperdicios nucleares
Manufactura critica	Servicios de emergencia	Instalaciones gubernamentales	Sistemas de transporte
Comunicaciones	Energía	Sanidad y salud pública	Sistema de agua y alcantarillado

Nota. Identificación de los 16 sectores de infraestructura crítica en la política presidencial 21(PPD-21).

Las barreras respecto a la ciberseguridad industrial requieren mayor aseguramiento debido a que las operaciones industriales son críticas; convertir buenas intenciones en acción puede ser un desafío principalmente por dos razones: primero, las redes industriales a menudo son administradas por equipos de TO que no tienen habilidades avanzadas de ciberseguridad, también pueden estar preocupados de que el equipo de TI tome medidas que reduzcan el tiempo de actividad operativo, a diferencia de una interrupción de 2 horas en un servidor de correo electrónico cuyos costos se miden en términos de pérdida de productividad y molestias, una interrupción no planificada de 2 horas en una línea de ensamblaje puede detener la producción y los ingresos de la compañía, la segunda razón es la barrera de no saber por dónde empezar, las redes industriales son muy complejas [11].

Dentro de los desafíos de ciberseguridad para IoT se encuentra un gran número de dispositivos con capacidades limitadas, vulnerabilidades, amenazas cibernéticas, integración con otras tecnologías emergentes, velocidad del almacenamiento de datos y conexión unidireccional de los equipos, también se identifica que IoT presenta falta de visibilidad y consciencia pública para protegerse de amenazas priorizando la disponibilidad, la integridad y finalmente la confidencialidad de los datos [12]. Por lo anterior, se vienen desarrollando marcos de referencia con políticas de ciberseguridad y de tecnología de IoT que identifican oportunidades de negocio y crean valor organizacional [13].

Para apoyar los procesos anteriormente mencionados, se abordan diferentes tipos de estándares y metodologías que dan flexibilidad a la investigación en curso; hay metodologías de certificación de seguridad aplicada para IoT, las cuales cuentan como un reto de seguridad amplio por la heterogeneidad de

dispositivos y por la identificación los ataques, es por esto que se plantean como solución marcos de referencia basados en estándares internacionales como ISO,ISA y NIST, sin embargo aún con esto no se resuelve el problema de privacidad y de riesgos, si los estándares y metodologías para proteger la tecnología no son respetados o son mal manejados por las organizaciones, pueden presentarse brechas de seguridad que desencadenen riesgos potenciales [14].

A nivel mundial existen diferentes estándares o marcos de referencia enfocados a la ciberseguridad tales como: ISO/IEC 27001 - 27002, NIST CSF e ISA 99/IEC62443 los cuales están orientados a la problemática de la ciberseguridad que apoyan en la presente investigación [15]. La aproximación basada en zonas, conductos y niveles de seguridad del estándar IEC62443 bajo el modelo de Pardue, permite establecer una base sólida de protección de los sistemas de operación y de información del entorno industrial de una forma ágil, también proporciona un lenguaje común entre los propietarios, los integradores y los fabricantes de tecnología que permite establecer una buena comunicación para dirigirse a los requisitos de protección de los entornos de automatización y control industrial [16].

En Colombia, el Gobierno Nacional publicó para comentarios el documento borrador del decreto de ciberseguridad, que tiene por objeto: "Reglamentar parcialmente los artículos 147 y 230 de la Ley 1450 de 2011, modificado por el artículo 148 de la Ley 1955 de 2019 y el artículo 64 de la Ley 1437 de 2011, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital" [17].

MARCO CONCEPTUAL

El término industria textil se define en principio al tejido de telas a partir de fibras, pero en la actualidad abarca una amplia gama de procesos, como el punto, el tufting o anudado de alfombras el cual es un tipo de fabricación textil en la que se inserta un hilo sobre una base primaria, el enfurtido, entre otros. Incluye también el hilado a partir de fibras sintéticas o naturales y el acabado y la tinción de tejidos. Esta industria se encuentra al interior del sector manufacturero, el cual se define como aquellas actividades representadas por la transformación continua y a gran escala de materias primas en productos transformables [18].

A lo largo de la historia, se ha mencionado que el desarrollo tecnológico en los últimos años ha tenido un impacto importante en los sistemas de producción, primero con la máquina de vapor y la mecanización de los procesos, luego con la producción en masa, la automatización y la robótica; recientemente ha sido llamada industria 4.0 y es considerada como la cuarta revolución industrial debido a su gran potencial y beneficios relacionados con la integración, la innovación y la autonomía de los procesos industriales que permitan crear una competencia global exigente para los entornos productivos y los obliga a reconfigurar sus procesos con el fin de acelerar la transformación digital y la innovación de la tecnología [19]. Por otro lado, se ha incursionado el concepto de industria 4.0 en la revolución digital la cual ha sido impulsada por el IoT también conocido como Internet de las cosas, que permite llevar la transformación digital a otro nivel. Se evidencia que la revolución industrial que se aproxima no tiene precedentes, ahora las máquinas están generando redes sociales propias para comunicarse entre sí, y así poder comunicarse con las personas, es una integración que reducirá costos para las empresas y permitirá una mayor eficiencia operativa; así

mismo, se traza un camino que trae competitividad y permite prepararnos para ver la industria 4.0 en Colombia [3].

La Ciberseguridad Industrial es el conjunto de prácticas, procesos y tecnologías diseñadas para gestionar el riesgo del ciberespacio derivado del uso, procesamiento, almacenamiento y transmisión de información en las organizaciones e infraestructuras industriales. Se enfoca en las perspectivas de personas, procesos y tecnologías. Sin embargo, es importante tener en cuenta que la Ciberseguridad Industrial debe complementarse con otras dimensiones de la seguridad, como la seguridad medioambiental, la seguridad física y la seguridad de las personas y el equipamiento. Además, es crucial considerar y proteger el patrimonio tecnológico de las industrias, que comprende activos tangibles e intangibles. Este patrimonio puede incluir ideas, invenciones, secretos industriales, procesos, programas, datos, fórmulas, patentes, derechos de autor, marcas o aplicaciones. No siempre se clasificará como una infraestructura crítica, dependiendo del sector al que pertenezca, pero siempre será el activo principal a proteger por parte de las industrias [1].

La introducción y el avance con las nuevas tecnologías de comunicación ha permitido pasar de los sistemas centralizados caracterizados por altas prestaciones y costos elevados a sistemas descentralizados o distribuidos los cuales están basados en equipos más sencillos conectados a las redes de comunicación [20]. Los dispositivos IoT que componen los sistemas TO constituyen la internet de las cosas; IoT es definido como todo objeto físico o dispositivo inteligente, con capacidades de computación, es decir, que dispone de electrónica y/o de un ordenador embebido (habitualmente de reducido tamaño), y con capacidades de interconexión con redes de datos, ya sean internas o a internet permitiendo que estos equipos puedan interactuar entre ellos usando protocolos estándares o propietarios los cuales podrían analizar los datos para prever errores, autoconfigurarse y adaptarse a posibles cambio; con la adopción de IoT se incrementa notablemente el volumen de datos generados, para soportar esto se necesitan tecnologías y sistemas diseñados para recopilar, almacenar y analizar de manera efectiva la cantidad de datos para luego interactuar con la información y generar valor a la organización [21].

Como consecuencia de la nuevas tecnologías de la comunicación, IoT es una serie de dispositivos inteligentes en red que están equipados con microchips, sensores y dispositivos inalámbricos con capacidades de comunicaciones los cuales presentan constantemente aumentos de potencia de procesamiento, capacidades de almacenamiento y capacidades de conectividad que presentan mayor reducción en los tamaños de sus componentes y baja de precio lo cual les permite posicionarse como elementos indispensables para las tecnologías de la fabricación inteligente [6]. Así mismo, empresas líderes en el mercado indican que el IoT hace referencia a los objetos cotidianos que se conectan a una red e intercambian datos con otros dispositivos, pero el IIoT es una parte del IoT que por lo general comprende cualquier equipo que aprovecha la conexión a Internet para enviar o recibir datos, pero cuando se utilizan con fines industriales, se les considera IIoT [22].

Por consiguiente, debido a la convergencia que están teniendo los sistemas TO y TI, están expuestos a un panorama de amenazas en expansión que no se había evidenciado; las plataformas TO son objetivos para los hackers involucrados en el terrorismo, la guerra cibernética y el espionaje pero hay un panorama de amenazas que agrava más el riesgo y es debido a que los líderes de TO no utilizan las mejores prácticas de seguridad las cuales pueden brindar la adaptabilidad y la flexibilidad necesaria para que sus equipos de

trabajo lleguen al éxito, junto con la planificación anticipada para asegurarse que la productividad no se vea afectada; a medida que las organizaciones enfrentan mayores amenazas y vulnerabilidades, bajos presupuestos y escases de personal, los líderes de TO tendrán cada día la tarea de adaptarse y reinventarse para garantizar la correcta operación de los activos industriales [7].

Por la criticidad del ambiente TO y el aumento de la cantidad de incidentes de ciberseguridad, se empezaron a consolidar los estándares de seguridad industrial como herramientas para fomentar la disponibilidad y tolerancia a fallos en los sistemas. Existen diferentes estándares que impactan la ciberseguridad como ISA 99/IEC62443, ISO 27001, ISO 27002, NIST 800-82 [9]. Los especialistas del entorno TI se enfocan en la serie de los estándares ISO 27001 mientras que los especialistas del entorno TO tienden a preferir las normas IEC 62443 y NIST 800-82; aunque los requisitos de seguridad informática son globales, se evidencia que la criticidad de los requisitos de las áreas de la operación es diferente a los del ambiente TI, esto se puede visualizar en la Tabla 2 [23].

Tabla 2. Diferencias entre los dominios TI y TO

Dominio	**Definición acorde al Grupo Gartner [GAR2021]**	**Ejemplos de aplicación**
TI	TI es el término utilizado para describir el rango completo de procesamiento de información, software, hardware, tecnologías de la información y tecnologías integradas	- Laptops - Servicios web - Servicios de correo - electrónico - Sistema SAP - Servicios de carpetas compartidas - Redes
TO	TO es el término utilizado para los elementos de hardware y software que detectan o provocan cambios a nivel de control en equipos industriales.	- PLC - Paneles táctiles - Servidores de control industrial - Robots industriales - Sistemas de entradas y salidas remotas - Redes en tiempo real

Nota. Se identifican las diferencias entre los entornos TI y TO basados en las definiciones de Gartner. Fuente: Adaptado [23].

El estándar ISO 27001 se enfoca en el establecimiento y operación de un SGSI, esta norma define los requisitos escenciales para la organización en terminos de planificación, responsabilidades, evaluación de riesgos, comunicación, auditoría, entre otros; el estándar ISO 27002 define requisitos más especificos para la seguridad de TI como el control de acceso y la seguridad de la red; por su lado, el estándar IEC 62443 se centra en la protección de los sistemas industriales y todo lo relacionado con tecnologías de la operación [23].

MARCO REFERENCIAL

En los últimos años, ha habido un crecimiento significativo de la conectividad de los dispositivos electrónicos industriales. Cada vez más dispositivos están interconectados, lo que ha llevado a la digitalización de muchos procesos y ha abierto un mundo de posibilidades. Sin embargo, junto con estas oportunidades, también han surgido riesgos que deben ser abordados adecuadamente. Uno de los riesgos más importantes es la ciberseguridad, la cual se ha convertido en un elemento clave en las estrategias de seguridad nacional de muchos países. A medida que nuestras sociedades se vuelven más dependientes de la tecnología, los ciberataques pueden representar una amenaza significativa para la estabilidad y la seguridad de una nación. Los campos en los que se desarrolla la guerra han evolucionado más allá de los tradicionales dominios del aire, mar, tierra e incluso el espacio, y ahora incluyen una amplia variedad de amenazas que se materializan en el ciberespacio [24].

Los ambientes TI y TO se han administrado de manera independiente y se han comportado como entidades separadas dentro de una arquitectura organizacional que conlleva algunas excepciones entorno a los diferentes tipos de datos e informes que genera cada ambiente, el TI y el TO. Las redes corporativas, la nube y las operaciones conectadas se convierten en una base de arquitectura estándar enfocada en habilitar las aplicaciones del ambiente operacional el cual se identifica como un riesgo expuesto en el entorno TO por la convergencia que ha tenido en los últimos años [7]. Con lo anterior, se presentan nuevos riesgos que han llamado la atención de los niveles de las compañías, desde el equipo de seguridad, CIO, CISO, hasta la alta gerencia. El llamado “air gap” ahora está plagado de agujeros de seguridad como resultado de esta mayor conectividad de dispositivos TO, esto aumenta la necesidad de brindar un enfoque sólido para la seguridad. Hay tres puntos de interés que se deben revisar respecto a los problemas de seguridad en la tecnología operativa: capacidades débiles de ciberseguridad en las plataformas existentes, aplicación de parches y control de versiones indisciplinados de los sistemas TO e identificar que efectivamente los sistemas TO son blanco de ataque para los actores de amenazas conocidos [4].

Las amenazas en el ciberespacio obligan a los Estados a tomar medidas que antes no eran consideradas. La protección de los sistemas informáticos, la infraestructura crítica y los datos sensibles se ha convertido en una prioridad estratégica. Los Estados deben desarrollar políticas y regulaciones sólidas, así como invertir en capacidades técnicas y humanas para defenderse contra los ciberataques. La colaboración internacional también es crucial en el ámbito de la ciberseguridad. Dado que los ciberdelincuentes y los actores maliciosos no conocen fronteras, es fundamental que los países trabajen juntos para compartir información, intercambiar mejores prácticas y coordinar respuestas conjuntas. Solo a través de una cooperación estrecha y un enfoque integral, podremos hacer frente a los desafíos y salvaguardar la seguridad en el ciberespacio [24].

En la actualidad, la guía sobre controles de seguridad en sistemas TO indica que las plataformas TO padecen de los mismos males tradicionales de los sistemas TI debido a la convergencia y a la conectividad, así mismo se identifican las consecuencias de un mundo convergente, donde cada vez crece más la necesidad de mantener todos los dispositivos conectados, esto hace que las redes industriales comiencen a tener la necesidad de conectarse, utilizando protocolos como TCP, inseguros en su definición y encapsulando paquetes tradicionales de protocolos propietarios industriales como MODBUS; aunque una organización decida mantener estos sistemas TO desconectados de sus redes corporativas o de internet, los dispositivos

que se utilizan para configurar y mantener estos en operación, son portátiles, pendrives, tabletas y smartphones, que han tenido contacto previo con internet y con sistemas operativos Microsoft Windows, por lo que sigue existiendo riesgo si no se aplican políticas de seguridad [9].

Desarrolladores de tecnología sugieren centrarse en mejorar la visibilidad y la seguridad para que TI y TO puedan trabajar juntos con el fin de definir zonas de confianza, hacer cumplir la segmentación y monitorear los puntos finales tratando de identificar amenazas antes de que sea demasiado tarde, esto se logra realizando la segmentación la cual funciona controlando el flujo del tráfico entre las partes. Algunas tecnologías tradicionales para la segmentación incluían cortafuegos internos, configuraciones de ACL y VLAN's en equipos de red. Sin embargo, estos enfoques son costosos y difíciles por lo cual propone la tecnología de acceso definida por software debido a que simplifica la segmentación al agrupar y etiquetar el tráfico de red, posterior a esto utiliza etiquetas de tráfico para hacer cumplir la política de segmentación directamente en el equipo de la red, pero sin la complejidad de los enfoques tradicionales [11].

La seguridad cibernética es crítica, en el entorno TI ayuda a las organizaciones a mantener seguros los datos confidenciales, ayuda a garantizar que los usuarios se conecten a Internet de forma segura y detectar y prevenir posibles ataques cibernéticos pero, el entorno TO también requiere un esquema de ciberseguridad similar que permita proteger la infraestructura crítica; cualquier retraso momentáneo o período de tiempo de inactividad no planificado puede hacer que las plantas de fabricación, las centrales eléctricas o los sistemas de suministro de agua presenten errores en el suministro de los servicios o se apaguen [7]. En este mismo sentido, la ciberseguridad se ha convertido en un asunto global, las protecciones o controles que se deben utilizar contra las actividades delictivas ha terminado siendo un asunto complicado para todas las naciones, sectores e industrias, es por esto que se plantean discusiones sobre la regulación del ciberespacio, la gobernanza y la defensa unilateral debido a la cantidad de incidentes críticos que se han presentado a nivel internacional en los últimos años (ver *Tabla* 3) [25].

Tabla 3. Incidentes cibernéticos internacionales

Año	**Incidente**
2003	Acusación de EEUU a China sobre ataques informáticos (Titan Rain)
2007	Ataques a Estonia que inutilizaron infraestructuras críticas
2008	Explosión por ataque Cibernético en oleoducto BTC en Refahiye-Turquía
2010	El gusano informático Stuxnet genera daños en plantas de uranio y sabotea proyectos estratégicos nacionales
2012	Borrado de 30.000 discos duros de la empresa petrolera Aaudí Aramco
2016	Presunto ciberataque ruso en las elecciones presidenciales de EEUU con filtraciones de información de los servidores de correo del Comité Nacional Demócrata y de su candidata Hilary Clinton, publicación de documentos para afectar su imagen y posible manipulación de elecciones en favor de Donald Trump
2018	Supuestos ciberataques contra estructuras de información de Rusia en la copa mundial de futbol contra redes de suministro eléctrico
2019	Presuntos ataques cibernéticos a la infraestructura eléctrica de Venezuela
2020	Acusaciones entre potencias por presuntos ataques cibernéticos para robo de propiedad intelectual e información sobre vacunas COVID19
2020	Intrusión a la plataforma de videoconferencias Zoom para extraer información, infiltrar datos y acceder a reuniones remotas.
2021	Los ciberdelincuentes lograron acceder a los sistemas de SolarWinds y utilizaron su software para distribuir malware a miles de empresas y organizaciones en todo el mundo.

2021	Un grupo de hackers chinos habían estado explotando vulnerabilidades en el servidor de correo electrónico Microsoft Exchange para acceder a los datos de empresas y organizaciones en todo el mundo.
2021	Un grupo de hackers conocido como DarkSide atacó Colonial Pipeline, uno de los principales operadores de oleoductos en los Estados Unidos. El ataque paralizó la operación de la empresa y provocó una escasez de gasolina en la costa este de los Estados Unidos.
2022	Una planta de producción de automóviles en América del Norte fue atacada por un grupo de ransomware, lo que causó interrupciones en la producción y la distribución de vehículos.
2022	Una red de transporte público en Europa fue atacada por un grupo de ransomware, lo que causó interrupciones en los servicios de transporte y la emisión de billetes.
2022	Una central eléctrica en Europa fue atacada por un grupo de hackers, lo que causó interrupciones en la producción y la distribución de energía.

Nota. Listado de incidentes cibernéticos entre el año 2003 y 2022. Fuente: Adaptado [26].

El estudio anual Cyber Resilient Organization identifica que un 77% de las organizaciones no están preparadas para enfrentar los ataques cibernéticos y que tampoco tienen un plan consistente de respuesta ante dichas amenazas teniendo claro que actualmente hay estándares, protocolos, métodos, reglas, herramientas y normas que ayudan a minimizar los riesgos y las amenazas apoyados en software y hardware [25]. El gobierno español a través de su ministerio del interior ha determinado que es normal que existan instalaciones industriales soportadas por sistemas operativos y hardware que no cuentan con soporte vigente debido a que se implementaron hace muchos años y son necesarios para la operación, seamos o no consientes de esto, el problema es crítico, toda vez que se juntan dos entornos, TI y TO los cuales presentan diferentes necesidades de conocimiento y ciclos de vida muy diferentes que complican el establecimiento de prioridades a la hora de mitigar el riesgo de ciberataques en las organizaciones, enfrentándonos a grandes retos debido a la incorporación de dispositivos industriales de infraestructura crítica los cuales no están debidamente formados, se desconocen los riesgos y no hay esfuerzos entre TI y TO para aplicar medidas y controles de seguridad [9].

Las plataformas TO son vinculadas a servicios y tecnologías muy específicas las cuales requieren especialistas que necesitan interconexión con las plataformas pero muchas organizaciones del ámbito industrial no poseen una cultura de ciberseguridad ni cuenta con áreas expertas en el tema que les pueda apoyar en dar una mejor gestión a este tipo de escenarios, esto implica que los sistemas sean accedidos por personal externo especializado lo cual puede traer como consecuencias prácticas inseguras como filtración de información crítica para el negocio, exposición de información, explotación de vulnerabilidades que pongan en riesgo la infraestructura TO, en resumen, se está expuesto a los mismos riesgos del entorno TI pero agravados por la propia naturaleza de los entornos TO [9].

Las redes TO gestionan procesos industriales los cuales se están digitalizando gracias a la incorporación de soluciones de IoT, es necesario tener en cuenta aspectos relacionados con la privacidad cuyo ámbito esté regulado por las políticas gubernamentales; en este escenario los dispositivos inteligentes que automatizan procesos y generan gran cantidad de información deben plantear la revisión del concepto de privacidad en este tipo de entornos debido a que hay recolección de datos personales de los usuarios inherentes a la operación, esto obliga a que estemos inmersos en un ambiente de riesgos y amenazas donde se deben contemplar controles orientados a preservar la privacidad de los activos industriales desde el proceso de diseño, operación y gestión de los sistemas de la organización, así se alcanzará un marco de protección

integral [9]. En efecto, el IoT al ser una tecnología emergente tienen puntos de mejora respecto a la seguridad, a las políticas, a los estándares y al ámbito tecnológico que, de aplicarse correctamente, se puede empezar a garantizar el correcto procesamiento de datos y la entrega oportuna a los diferentes sistemas [5].

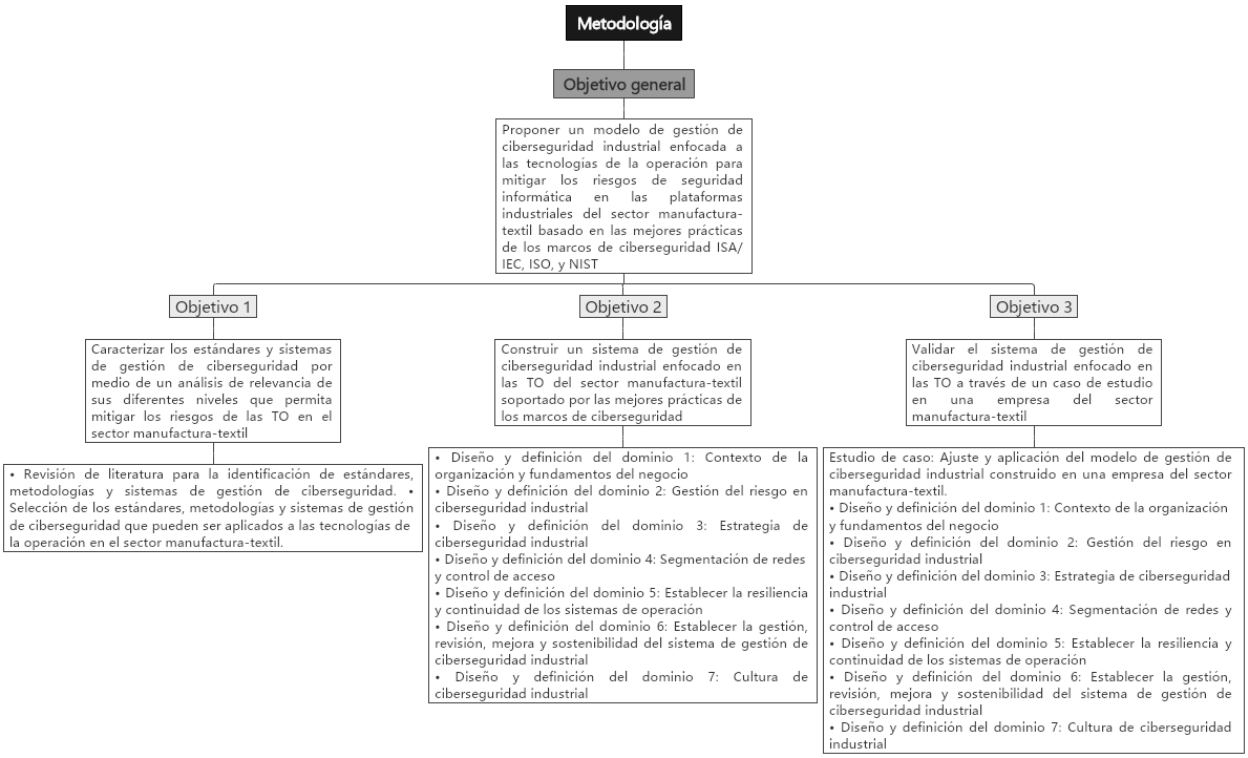
Así mismo, cada vez son más las infraestructuras críticas que sufren explotaciones por tener dispositivos IoT conectados a las redes sin ningún tipo de control, basta con ejecutar búsquedas en shodan.io, herramienta para el reconocimiento pasivo y se podrá identificar la gran cantidad de equipos ICS (Sistemas de control industrial) conectados a internet sin ningún tipo de restricción, igualmente se puede consultar a la MITRE for ICS y se identificará la cantidad de amenazas a las que estos sistemas están expuestas; la automatización industrial no es nueva, este tipo de sistemas de control industrial existen desde hace mucho tiempo y operan correctamente, el punto crítico es que están migrando a redes TCP/IP y es por esto que están en el foco de atención, ya no son plataformas aisladas, ahora están interconectadas por lo que se vuelven atractivas para organizaciones criminales que tienen capacidades y el conocimiento suficiente para acceder y tomar control de este tipo de sistemas utilizando malware especializado [9].

En la industria manufacturera del sector textil se utilizan sistemas SCADA, se han observado ataques que afectan la disponibilidad, confidencialidad e integridad de los sistemas. Para mitigar estos riesgos, es necesario tener herramientas adecuadas como los sistemas de gestión de ciberseguridad, que ayuden a determinar el nivel de madurez de la seguridad de la información en el sector textil. Esto implica identificar, evaluar y calificar los elementos de seguridad que pueden generar los riesgos asociados a la seguridad. Al identificar cada uno de los elementos que intervienen en los procesos de estos sistemas, es posible comprender su relación, dependencia e importancia, lo que permite identificar el impacto que pueden ocasionar en los factores de seguridad. Una vez que se tiene conocimiento de las debilidades en los controles de seguridad, se pueden establecer estrategias para mitigar las vulnerabilidades presentes en estos sistemas, fortaleciendo así el estado de madurez de los procesos y actividades que se llevan a cabo en ellos [27].

METODOLOGÍA

La metodología aplicada para la construcción del modelo de gestión de ciberseguridad industrial enfocado en las tecnologías de la operación para mitigar los riesgos de seguridad informática en las plataformas industriales del sector manufactura-textil es de tipo cualitativa, la cual permite comprender los fenómenos en cuestión explorándolos desde la perspectiva del ambiente natural debido a que el tema en TO no ha sido tan explorado y aplicado como en el ambiente TI. Esta metodología permitió comprender y resolver la problemática específica aplicando la teoría y las mejores prácticas de acuerdo con el planteamiento del problema de investigación; adicionalmente se realizó un estudio de caso, el cual permitió tener un escenario de validación y de experimentación en una empresa del sector manufactura-textil [28]. En la *Figura 2*, se presenta el diagrama metodológico que detalla los pasos aplicados en el desarrollo de este estudio para la construcción del modelo.

Figura 2. Metodología



Nota. Se plantearon las actividades a ejecutar para cada uno de los objetivos de la investigación. Fuente: Elaboración propia.

En la metodología propuesta en la *Figura 2*, se propusieron diferentes fases las cuales se acompañan de las actividades ejecutadas. A continuación, se comparte el detalle de cada una de ellas.

Fase I: Estándares y sistemas de gestión de ciberseguridad.

Se identificaron y se caracterizaron las principales fuentes de los estándares y sistemas de gestión de ciberseguridad, para ello se realizó una búsqueda en la literatura que apoya el problema en cuestión. La realización de esta búsqueda permitió identificar las últimas tendencias que recomiendan los fabricantes de tecnología, las academias y los estándares universales. Adicionalmente, permitió seleccionar los frameworks de gestión de ciberseguridad que más se ajustan a la presente investigación donde no se encuentra un estándar a nivel industrial pertinente a las necesidades manifiestas del sector, permitiendo así, generar el análisis de relevancia entre los diferentes frameworks y darle continuidad a la fase II que se enfoca en la construcción del sistema de gestión de ciberseguridad industrial.

Fase II: Construcción del sistema de gestión de ciberseguridad Industrial.

Se construyó el sistema de gestión de ciberseguridad industrial enfocado en las tecnologías de la operación del sector manufactura-textil, para ello se utilizaron las mejores prácticas de los estándares y sistemas de gestión seleccionados en la fase I. Adicionalmente, se construyeron los diferentes dominios que conforman

el sistema de gestión de ciberseguridad, logrando una sólida base para la mitigación de riesgos en el sector manufactura-textil.

Fase III: Validación del sistema de gestión de ciberseguridad industrial.

Se realizaron los ajustes al sistema de gestión de ciberseguridad industrial construido y se validó en una empresa del sector manufactura-textil. Esta fase permitió validar la eficacia del modelo propuesto para mitigar los riesgos de ciberseguridad industrial. Finalmente, se realizaron las respectivas conclusiones de la validación del sistema y los hallazgos encontrados.

EJECUCIÓN DE LA METODOLOGÍA Y RESULTADOS
FASE I - ESTÁNDARES Y SISTEMAS DE GESTIÓN DE CIBERSEGURIDAD.

A. Revisión de literatura para la identificación de estándares, metodologías y sistemas de gestión de ciberseguridad.

Los modelos de seguridad y de maduración de ciberseguridad son complejos de implementar, tampoco son adecuados para planes personalizados y no consideran características organizacionales [29]. No es posible acceder a un nivel de protección total respecto a la explotación cibernética pero es fundamental la implementación de los SGSI con el fin de contribuir a que los riesgos sean conocidos, asumidos, gestionados y mitigados de forma organizada, eficiente y adaptada al entorno y a las políticas TIC's, adicionalmente estos sistemas de gestión deben contemplar diferentes elementos como el manual de seguridad, los procedimientos, las instrucciones, la lista de chequeo, los formularios y los registros de información que deben garantizar el ciclo PHVA (planear, hacer, verificar y actuar) para su base de implementación y gestión el cual puede o no integrarse con otras plataformas de calidad como ISO 9001, ISO 14001 e ISO 4500 [25].

Las organizaciones encargadas de establecer estándares de seguridad de la información han trabajado para adaptar sus directrices a los requisitos de los Sistemas de Control Industrial (ICS, por sus siglas en inglés). Sin embargo, esta adaptación ha dado lugar a intensos debates entre aquellos que respaldan la idea de mantener una segregación clara entre las Tecnologías de la Información (TI) y las Tecnologías Operativas (TO), y que no están de acuerdo con la implementación de estándares y directrices que se generaron originalmente para las TI. Estas discusiones se basan en diferentes puntos de vista sobre cómo se deben abordar los desafíos de seguridad en los entornos ICS. Algunos fabricantes argumentan que los estándares de seguridad de la información diseñados para las TI pueden no ser aplicables o adecuados para los sistemas de control industrial, ya que las TO tienen requisitos y características específicas que los diferencian de las TI. Por lo tanto, defienden la idea de mantener una separación estricta entre las dos áreas, evitando la aplicación de estándares y directrices originalmente concebidos para las TI en los entornos TO[24].

Algunos fabricantes indican que los estándares de seguridad de la información pueden ser adaptados y aplicados de manera efectiva a los entornos ICS, estos argumentan que muchos de los principios y prácticas fundamentales de la seguridad de la información son igualmente relevantes y necesarios tanto para las TI como para las TO, sosteniendo que la convergencia entre estos ambientes es inevitable en un mundo cada

vez más interconectado, y que la aplicación de estándares comunes puede facilitar la gestión y protección de los sistemas industriales. En última instancia, esta discusión refleja la complejidad y los desafíos que implica la seguridad de la información en los entornos ICS. A medida que la tecnología avanza y los sistemas se vuelven más interconectados, es necesario encontrar un equilibrio entre la adopción de estándares y directrices que han demostrado ser efectivos en las TI, y la consideración de las particularidades y requisitos específicos de las TO. La colaboración y el diálogo continuo entre las partes interesadas son fundamentales para avanzar hacia enfoques de seguridad que aborden de manera integral y efectiva las necesidades de los sistemas de control industrial [24].

Con la introducción de las regulaciones de la industria, diferentes organizaciones han creado estructuras y marcos de referencia entorno a las mejores prácticas de la seguridad empresarial y han conformado conjuntos de marcos de seguridad cibernética. En la *Tabla* 5 se visualizan los frameworks más utilizados a nivel mundial, esta información apoya directamente el análisis de relevancia de la presente investigación [30].

Tabla 4. Identificación de los principales marcos de referencia

Marco de referencia	Desarrollado por	Industria
NIST CSF	NIST	Infraestructura de operaciones críticas
ISO/IEC 27000	ISO 27001	Empresas en general
NIST SP 800-53	NIST	Agencias federales
CSA CCM	CSA	Proveedores de servicios en nube
ANSI/ISA-62443	ISA ANSI	Sistemas de control y automatización industrial
HITRUST CSF	HITRUST	Proveedores de servicios de salud
NERC CIP	NERC	Sistemas eléctricos

Nota. Se identifican los diferentes marcos de referencia y sus enfoques. Fuente: Adaptado [23].

A continuación, se explican los marcos de referencia identificados en la *Tabla* 5, adicionalmente se indica si apoya o no la presente investigación:

El CSA Security Trust Assurance and Risk (STAR) es un marco de seguridad de la información que proporciona una serie de controles y medidas de seguridad para ayudar a las empresas a evaluar, medir y gestionar los riesgos asociados con el uso de servicios en la nube. El marco se divide en tres áreas principales:

- Control: El marco proporciona un conjunto de controles de seguridad para la nube que se pueden utilizar para evaluar y medir el nivel de seguridad de los servicios en la nube. Estos controles se agrupan en categorías como gestión de identidad y acceso, seguridad de la red, seguridad de la aplicación, seguridad de los datos, etc.

- Medición: El marco proporciona una serie de herramientas y métodos para medir el nivel de seguridad de los servicios en la nube, como pruebas de penetración, evaluaciones de vulnerabilidades y análisis de riesgos.

- Gobierno: El marco proporciona orientación sobre cómo establecer y gestionar programas de gobierno de la seguridad de la información para garantizar que se tomen medidas adecuadas para proteger los datos y sistemas en la nube.

En resumen, CSA STAR es un marco útil para las empresas que deseen evaluar la seguridad de los servicios en la nube antes de adoptarlos y para los proveedores de servicios en la nube que deseen demostrar su compromiso con la seguridad de la información y la gestión de riesgos [31], sin embargo, en la presente investigación no abordaremos las plataformas en nube debido a que la empresa donde se realizará el caso de estudio no cuenta con servicios industriales en la nube.

HITRUST CSF (Health Information Trust Alliance Common Security Framework) es un marco de ciberseguridad creado específicamente para el sector de la salud. Fue diseñado para ayudar a las organizaciones de salud a abordar los desafíos únicos de seguridad y privacidad de los datos médicos. El marco consta de una serie de controles de seguridad y prácticas recomendadas que abarcan todas las áreas de seguridad de la información, incluyendo la gestión de riesgos, la seguridad de la red, la gestión de identidad y acceso, la seguridad física, la gestión de incidentes, la privacidad y otros. El HITRUST CSF utiliza un enfoque de riesgo basado en el cumplimiento normativo y utiliza un sistema de puntuación para evaluar el nivel de madurez de los controles de seguridad implementados en una organización. También proporciona una lista de requisitos de cumplimiento que abarca todas las leyes y regulaciones aplicables al sector de la salud, como HIPAA y HITECH.
El HITRUST CSF es un marco de ciberseguridad ampliamente utilizado en el sector de la salud enfocado en la evaluación y gestión de riesgos de seguridad en el sector[32]. Dado su enfoque en el sector salud, no se tendrá en cuenta para la presente investigación.

El NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) es un marco de ciberseguridad diseñado para proteger los sistemas críticos de la infraestructura eléctrica de Norteamérica. El marco consta de una serie de estándares y requisitos de seguridad que las empresas eléctricas deben cumplir para proteger sus sistemas críticos contra ciberataques. Los requisitos de seguridad abarcan áreas como la gestión de identidad y acceso, la seguridad de la red, la gestión de vulnerabilidades, la monitorización de eventos de seguridad, la gestión de incidentes y la recuperación de desastres. El NERC CIP utiliza un enfoque de evaluación de riesgos basado en el nivel de impacto que tendría un ciberataque en la infraestructura eléctrica crítica. El marco también incluye requisitos de cumplimiento y obligaciones de informes regulares que deben ser presentados a las autoridades reguladoras. El NERC CIP es un marco

de ciberseguridad muy importante para el sector eléctrico de Norteamérica y es considerado uno de los estándares más relevantes para la gestión de riesgos de ciberseguridad en el sector[33]. Debido a su enfoque en infraestructura eléctrica, este marco de referencia no será tenido en cuenta para la presente investigación.

El estándar NIST 800-82 aborda la seguridad en los sistemas de control industrial, proporciona una visión general de los sistemas y las topologías típicas identificando amenazas y vulnerabilidades, así como contramedidas de seguridad que nos permiten mitigar el impacto ante la explotación de vulnerabilidades en el entorno TO, se identifica que estos estándares apoyan totalmente la solución del problema planteado debido a que velan por la ciberseguridad de ambientes industriales [9]. El marco NIST CSF (framework cybersecurity) es un estándar de ciberseguridad ampliamente utilizado a nivel internacional, su misión va más allá de atender las necesidades de seguridad de las organizaciones individuales; este estándar se estableció con el fin de desarrollar infraestructuras de resiliencia cibernética para mantener los entornos seguros y protegidos, este marco ayuda a una organización a comenzar o mejorar su programa de ciberseguridad promoviendo la comunicación entre las partes interesadas internas y externas, adicionalmente, en las organizaciones más grandes, ayuda a integrar y alinear mejor los riesgos de ciberseguridad con los procesos más amplios de gestión de riesgo empresarial enumerando 5 funciones importantes para proporcionar una visión integral del ciclo de vida para la gestión de riesgos de ciberseguridad identificados en la *Figura* 2 [34].

Figura 3. Primeros pasos de NIST Marco de ciberseguridad

Nota. Guía de inicio rápido estándar NIST. Fuente: Adaptado [34]

Las actividades enumeradas a continuación por NIST proponen un punto inicial para las organizaciones con el fin de implementar el estándar [35]:

- Identificar:
    - Los procesos y activos críticos empresariales.
    - Flujos de información de documentos.

- Inventario de hardware y software.
- Establecer políticas para la ciberseguridad que incluya roles y responsabilidades.
- Amenazas, vulnerabilidades y riesgos a activos.

- Proteger:
  - Gestionar el acceso a activos de información.
  - Proteger los datos sensibles.

- Detectar:
  - Probar y actualizar los procesos de detección.
  - Hacer respaldos con regularidad.
  - Proteger los dispositivos.
  - Gestionar las vulnerabilidades de los dispositivos.
  - Capacitar a los usuarios.
  - Conocer los flujos de datos esperados de la empresa.
  - Mantener y monitorear los archivos de registro.

- Responder:
  - Asegurar que los planes de respuesta sean probados.
  - Asegurar que los planes de respuesta sean actualizados.

- Recuperar:
  - Comunicarse con las partes interesadas internas y externas.
  - Comprender el efecto de los eventos de ciberseguridad.
  - Coordinar las partes interesadas externas y externas.
  - Asegurar que los planes de recuperación sean actualizados.
  - Gestionar las relaciones públicas y la reputación de la compañía.

El marco NIST CSF tiene varias limitaciones respecto a su implementación, si bien el framework permite a las organizaciones, independientemente de su tamaño, de tipo y de grado de sofisticación en ciberseguridad, aplicar los principios y las mejores prácticas para la gestión de riesgos no es un esfuerzo trivial de emprender, NIST CSF permite que el líder de TI se califique a sí mismo en cada uno de los estándares establecidos, pero no especifica calificaciones aceptables para esos estándares es por esto que puede ser complementado con otro estándar que permita calificaciones más efectivas[34].

El marco de referencia de NIST es un lenguaje común para entender, manejar y expresar los riesgos de ciberseguridad externos e internos al igual que identifica y prioriza las acciones para reducir los riesgos en cualquier tipo de organización [29]. Este marco apoya considerablemente la investigación en cuestión, pues

ayuda en la identificación de activos y priorización de actividades para mitigar los riesgos de ciberseguridad.

El marco ISO/IEC 27001:2013 pertenece a la familia de normas ISO 27000 publicado en 2013 por la ISO y la IEC, este marco ayuda a las organizaciones a gestionar la seguridad de sus activos de información proporcionando un marco de gestión para implementar un SGSI con el fin de garantizar la confidencialidad, integridad y disponibilidad de todos los datos corporativos[36].

Un sistema de gestión de seguridad de la información es un sistema definido y documentado que consta de un conjunto de políticas, procesos y sistemas para gestionar los riesgos de los datos de la organización para garantizar niveles aceptables de riesgo de seguridad de la información, las evaluaciones de riesgos en curso ayudan a identificar las amenazas y vulnerabilidades de seguridad que deben administrarse a través de un conjunto de controles, adicionalmente, tener un SGSI establecido que cumpla con la norma ISO 27001 ayuda a administrar la confidencialidad, la integridad y la disponibilidad de todos los datos corporativos de una manera optimizada y rentable. A medida que se actualizaron los SGSI surgió una actualización llamada ISO/IEC 27002:2013 la cual se focaliza en habilitar referencias para la implementación de controles de seguridad como parte de los SGSI y cumple con ISO/IEC 27001:2013. En la *Tabla* 6 se identifican los beneficios de la certificación [36].

Tabla 5. Beneficios de la certificación ISO 27001

Proteja sus datos donde quiera que estén Un SGSI que cumple con la norma ISO 27001 ayuda a proteger todas las formas de información ya sea digital, en papel o en la nube	**Defiéndete de los ciberataques** La implementación y el mantenimiento de un SGSI reducirán significativamente los riesgos de seguridad cibernética y de filtración de datos de su organización
Reducir los costos de seguridad de la información Gracias al enfoque de evaluación y análisis de riesgos de un SGSI, las organizaciones pueden reducir los costos invertidos en agregar indiscriminadamente capas de tecnología defensiva que podrían no funcionar	**Responda a las amenazas de seguridad en evolución** Las organizaciones que cumplen con la norma ISO 27001 son más capaces de responder a los riesgos de la seguridad de la información en evolución debido a los requisitos de gestión de riesgos de la norma
Establecer una cultura de seguridad de la información Con ISO 27001 integrado en la cultura de la organización, los empleados son más conscientes de los riesgos de seguridad de la información y las medidas de seguridad tienen un amplio alance a todas las facetas de la organización	**Cumplir con las obligaciones contractuales** La certificación demuestra el compromiso de su organización con la seguridad de la información. Proporciona evidencia de que se ha comprometido formalmente a cumplir con las medidas de la seguridad de la información.

Nota. ISO 27001, la Norma Internacional de Seguridad de la Información. Fuente: Tomado [36]

La ISO/IEC 27002:2013 brinda pautas para los estándares de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización; el estándar está diseñado para ser utilizado por organizaciones que tienen la intención de seleccionar

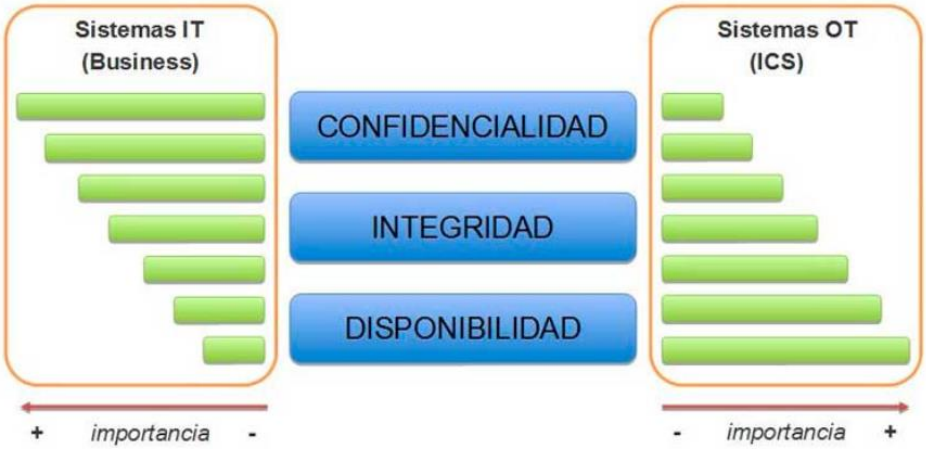
controles dentro del proceso de implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001, implementar controles de seguridad de la información comúnmente aceptados y desarrollar sus propias directrices de gestión de la seguridad de la información [37]. El presente marco apoya considerablemente la investigación en cuestión, ayuda a la implementación de los sistemas de gestión y a la implementación de controles que permitan mitigar los riesgos.

El estándar ISA 99/IEC62443 constituye el marco referencial internacional para la ciberseguridad de sistemas TO, los demás están enfocados principalmente en ambientes TI enmarcados en la seguridad de la información, este estándar identifica la disponibilidad y la integridad como elementos de suma importancia para el sector industrial, adicionalmente establece un ciclo de vida para la ciberseguridad industrial orientado en tres elementos: Evaluación, desarrollo e implementación y mantenimiento [9].
La ISA reunió el conjunto de estándares ISA99 para construir sistemas de control y automatización industrial seguros, IEC se basó en ese trabajo para presentar la IEC 62443 la cual corresponde a un marco para implementar las mejores prácticas de ciberseguridad industrial paso a paso, para la mejora continua; este estándar define una arquitectura de red segura, requisitos funcionales y pautas para medir su nivel de madurez para cada requisito donde TO aporta su conocimiento sobre qué activos necesitan comunicarse y qué tan críticos son, y TI aporta su experiencia y tecnología en ciberseguridad. Los estándares establecen un marco de cuatro pasos: Realice un inventario de activos, definir zonas, definir conductos y agregue controles para cada zona [11]. El estándar ISA99/IEC62443 constituye el principal marco de referencia internacional de ciberseguridad en sistemas industriales donde la disponibilidad y la integridad son los factores más importantes para la adopción de medidas de protección contra ciber amenazas, pero también para reducir los incidentes tecnológicos no intencionados; el comité ISA99 que desarrollo inicialmente el esquema IEC62443 está compuesto por una serie de miembros donde se encuentran propietarios, proveedores de equipamiento y servicios, gobiernos, instituciones educativas y diferentes grupos de investigación [16]. La metodología de ISA/IEC 62443 mejora la seguridad, confianza e integridad de los sistemas industriales basándose en procesos y considerando a las personas, el proceso de trabajo y la tecnología [38].

Para la presente investigación, se seleccionan las mejores prácticas de los estándares ISA 99/IEC62443, ISO 27001-2, NIST 800-82 para la construcción del SGCI, con este proyecto se contribuye a la mejora de la ciberseguridad industrial a través del desarrollo de actividades de análisis, desarrollo de estudios e intercambio de información sobre el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio en las organizaciones e infraestructuras industriales del sector manufactura-textil.

Es importante destacar que la ciberseguridad de TO, aunque se basa en los mismos pilares de la triada de ciberseguridad de TI, no se valora en los mismos niveles de criticidad, es decir, la ciberseguridad en el ambiente TI tiene como prioridad la confidencialidad, luego la integridad y por último la disponibilidad, a diferencia de la criticidad en el ambiente TO, donde la prioridad es la disponibilidad, posterior la integridad y por último la confidencialidad, esto puede visualizarse en la *Figura* 3 [9] [39].

Figura 4. Principios de seguridad TI vs TO

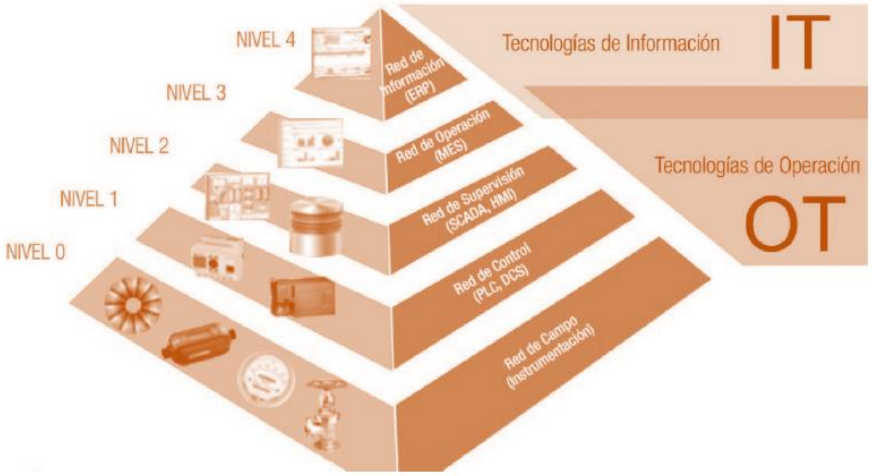


Nota. Ciberseguridad en la Industria 4.0 for dummies. Fuente: Tomado [39].

Para la gestión de la ciberseguridad en ICS, es importante establecer las mejores prácticas con el mayor nivel de detalle posible, dependiente de la realidad del entorno se recomienda adaptar las medidas a los diferentes niveles operacionales propuesto por el modelo de arquitectura PERA [9].

El Centro de Ciberseguridad Industrial se apoya en el modelo PERA, este modelo fue presentado por el marco ISA 95 y permite aplicar una separación basada en niveles los cuales están alineados con una pirámide de automatización que relaciona la convergencia entre el ambiente TI y el TO, este modelo es de la década de los 90s y sigue siendo aplicable hoy en día [40]. En este modelo se definen los componentes de una red TO en 4 niveles o capas las cuales se evidencian en la *Figura* 4. El nivel 0 corresponde a la adquisición de datos de campo o instrumentos, es decir, en este nivel están los sensores y los actuadores que se encuentran en todo el proceso y que permiten el control de las máquinas y los equipos de producción. El nivel 1 corresponde a la agrupación de los controladores locales como ordenadores, PLC's, entre otros, estos dispositivos utilizan los datos del proceso proporcionados por el nivel 0 y dan consignas a los actuadores. El nivel 2 corresponde a la supervisión con equipos destinados a controlar la secuencia de fabricación o producción, equipos como SCADA, estaciones operacionales o servidores de ingeniería. El nivel 3 corresponde a las operaciones de fabricación donde se gestionan los flujos de trabajo para producir u optimizar los productos finales y el nivel 4 corresponde a la gestión donde se desarrollan todas las actividades del negocio respecto al tema industriales, comunicando distintas plantas y manteniendo las relaciones con los proveedores y clientes [16]. El modelo PERA se tendrá en cuenta para introducirlo en el sistema de gestión de ciberseguridad industrial en uno de los dominios debido a su importancia a nivel industrial.

Figura 5. Ciberseguridad en la pirámide de automatización industrial



Nota. Componentes de una red TO Fuente: Tomado [9]

Los niveles de la *Figura* 5 fueron analizados y se identificaron diferentes vulnerabilidades al ser plataformas de TO. En la *Tabla* 6, se genera un listado con las principales vulnerabilidades que pueden estar presentes en cada uno de los niveles de la pirámide [16].

Tabla 6. Principales vulnerabilidades en los niveles de la pirámide de automatización industrial

	Niveles de la pirámide de Automatización Industrial				
Principales vulnerabilidades que pueden existir	**0**	**1**	**2**	**3**	**4**
Falta de medidas de seguridad física	*	*	*	*	*
Arquitectura de red insegura	*	*	*	*	*
Posibilidad de interceptar y alterar comportamiento de sensor	*				
Debilidad en los protocolos de comunicaciones	*	*	*	*	*
Instalación, configuración incorrecta o servicios innecesarios habilitados	*	*	*	*	
Falta de actualización de software		*	*	*	*
Fallos cero days	*	*	*	*	*
Almacenamiento sin protección		*	*	*	*
Debilidad frente a desbordamiento de buffer		*	*	*	*
Debilidad en identificación y autenticación (contraseñas)		*	*	*	
Asignación incorrecta de privilegios		*	*	*	*
Debilidad frente a Fuzzing (técnicas para proporcionar datos inválidos e inesperados)		*	*	*	
Debilidad frente a ataques de Cross-Site-Scripting			*	*	*
Debilidad frente a ejecución de código remoto			*	*	*
Personal de planta no capacitado en tecnologías de la operación e información	*	*	*	*	
Personal de TI no capacitado en tecnologías de la operación	*		*	*	*
Acuerdos de nivel de servicio insuficientes	*	*	*	*	*
Falta de control de cambios	*	*	*	*	*
Falta de planes de continuidad	*	*	*	*	*

Falta de procedimientos adecuados en el uso de tecnologías de la operación		*	*	*	
Personal contratado inadecuado o sin concientización o formación en ciberseguridad	*	*	*	*	*
Falta de mecanismos de monitorización	*	*	*	*	*
Conexiones públicas desprotegidas	*	*	*	*	*
Uso de herramientas de red no permitidas	*	*	*	*	*
Existencia de servidores dual home		*	*	*	*
Interfaz de acceso inadecuados			*	*	*
Documentación escasa	*	*	*	*	*
No realización de copias de seguridad (perdida de datos, ransomware…)		*	*	*	*
Carencia de software anti-malware		*	*	*	*
Utilización de usuarios genéricos		*	*	*	*

Nota. Matriz de vulnerabilidades que presentan los diferentes niveles de la automatización industrial. Fuente: Tomado [16].

El CCI define un sistema de gestión de ciberseguridad industrial cómo un conjunto de políticas, procedimientos, directrices y controles diseñados para proteger la infraestructura industrial y los activos críticos de ciber amenazas. Adicionalmente, para llevar a cabo el tratamiento eficaz, eficiente, continuo y alineado de los pilares a proteger (disponibilidad, integridad y confidenciales) en los sistemas industriales de control, el CCI sugiere basar el desarrollo en normas y estándares universales aceptados como marcos de referencia a nivel internacional lo cual refuerza las normas seleccionadas en la presente investigación.

Cómo se ha identificado, los estándares y sistemas de gestión de ciberseguridad son fundamentales para mitigar los riesgos de las TO en el sector, es por esto que para el desarrollo del primer objetivo específico "Caracterizar los estándares y sistemas de gestión de ciberseguridad por medio de un análisis de relevancia de sus diferentes niveles que permita mitigar los riesgos de las TO en el sector manufactura-textil" se realizó la revisión de literatura con el fin de identificar los diferentes estándares, metodologías y sistemas de gestión de ciberseguridad que apoyan la presente investigación. Lo anterior, permitió dar continuidad a la siguiente actividad que consiste en la generación del análisis de relevancia de los estándares enfocados en sistemas de gestión de ciberseguridad, esto, con el fin de seleccionar las mejores prácticas de cada uno de ellos, permitiendo consolidar un sistema de gestión de ciberseguridad industrial por medio de diferentes dominios que pueda ser aplicado al sector en cuestión. Cómo se identificó en la *Figura* 4, a nivel operacional el pilar de seguridad más importante es la disponibilidad, por lo cual, la norma más relevante en este nivel es la ISA/IEC 62443 debido a su enfoque industrial y operacional. A nivel táctico, se identificaron políticas y procedimientos de seguridad para la organización, esto proporciona orientación para proteger los sistemas de control industrial, el estándar más relevante para este nivel es la NIST 800-82. Finalmente, a nivel estratégico, se identificaron los requisitos, la implementación y el mejoramiento continuo del sistema de gestión, el estándar más relevante para este nivel es la ISO 27001/27002.

B. Selección de los estándares, metodologías y sistemas de gestión de ciberseguridad que pueden ser aplicados a las tecnologías de la operación en el sector manufactura-textil.

Los ataques cibernéticos dirigidos a infraestructuras críticas no pueden ser tratados simplemente como teorías o conceptos abstractos. Es crucial establecer planes de acción, hojas de ruta y sistemas de protección

concretos para enfrentar esta creciente amenaza. Las normas, estándares y guías existentes son referencias voluntarias que pueden ser aplicadas de manera amplia. Estas directrices proporcionan un lenguaje común y se centran en la gestión del riesgo, lo que ayuda a los responsables y operadores de infraestructuras críticas a identificar, catalogar y gestionar los riesgos relacionados con la seguridad informática.

Cuando se implementan medidas de seguridad basadas en los marcos de trabajo analizados, es importante tener una visión integral del sistema completo y aplicarlas a todos los niveles organizativos. Esto implica comenzar desde los niveles técnicos más bajos y avanzar hacia las medidas organizativas y de procesos que involucren a todas las personas dentro de la organización, desde los operarios hasta la alta gerencia.

La ciberseguridad debe ser una preocupación y responsabilidad compartida en toda la organización, no se trata solo de implementar medidas técnicas, sino también fomentar una cultura de seguridad industrial en todos los niveles. Esto implica concientizar y capacitar a todos los miembros del equipo, promover buenas prácticas de seguridad y garantizar que se sigan los protocolos y procedimientos establecidos.

En el análisis de la fase I, se identificaron los principales frameworks o modelos de referencia que apoyan directamente la presente investigación, esto es debido al enfoque de ciberseguridad el cual permite ser aplicado a la industria manufactura-textil. En la *Tabla* 8, se realiza el análisis de relevancia de estos frameworks permitiendo consolidar sus ventajas y desventajas para poder crear los diferentes dominios que integra el modelo de gestión de ciberseguridad industrial enfocado en el sector manufactura-textil.

Tabla 7. Análisis de relevancia entre los frameworks de ciberseguridad seleccionados

Norma / **Información**	**ISO 27001-27002**	**ISA/IEC 62443**	**NIST 800-82**
Descripción	Norma internacional emitida por la organización internacional de normalización que describe cómo gestionar la seguridad de la información en una empresa. Proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. Enfocado en tecnologías de la información.	Norma internacional emitida por la sociedad internacional de automatización (ISA) proporciona un marco flexible para abordar y mitigar las vulnerabilidades de seguridad actuales y futuras en los sistemas de control y automatización industrial enfocado en infraestructura crítica.	Norma internacional emitida por el instituto nacional de estándares y tecnología de usa, publica el documento de seguridad de sistemas de control industrial.

Alcance	Proporciona requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.	Proporciona seguridad de los sistemas de control y automatización industrial (IACS).	Proporciona orientación para proteger los sistemas de control industrial (ICS).
Ámbito de la aplicación	Es una norma de seguridad de la información general, que puede ser aplicada a todas las organizaciones independiente de su tamaño o enfoque	Es una norma que se centra específicamente en la ciberseguridad industrial y se enfoca en la protección de los sistemas de control y automatización	Es una norma que se aplica a los sistemas de control industrial y se enfoca en la protección de estos sistemas
Propone	• Pautas y requisitos para la implementación de un sistema de gestión de seguridad de la información. • Priorizar los requisitos de confidencialidad, integridad y disponibilidad • Ciclo PHVA para el control de calidad en los entornos de producción • Ciclo PHVA para ayudar a las organizaciones a establecer el contexto, definir el alcance, los objetivos, la experiencia requerida y una política documentada. • Controles de seguridad requeridos para minimizar riesgos frente a la seguridad de la información.	• Un marco para administrar y asegurar los sistemas TO • Requisitos técnicos de seguridad en los componentes • Requisitos de seguridad del sistema y niveles de seguridad • Lenguaje común para los proveedores de productos • Ciclo de vida de desarrollo seguro y mantenimiento de productos seguros • Evaluación de riesgos de seguridad. • Agrupar los activos similares tomando como referencia el modelo de Pardue basado en conductos y zonas de seguridad • Segmentación de redes internas en TO	• Guía para establecer seguridad en sistemas de control industrial. • Desarrollo de políticas de seguridad. • Política de programa. • Política de asuntos específicos. • Política de sistemas específicos. • Gestión y evaluación de riesgos del sistema de control industrial. • Arquitectura de seguridad del sistema de control industrial. • Aplicación de controles de seguridad a ICS.
Enfoque de gestión	Se enfoca en la planificación, implementación, monitoreo y mejora continua de los procesos de seguridad de la información en la organización	Se enfoca en la gestión de la ciberseguridad industrial, pero está más centrada en la identificación de riesgos, la evaluación de vulnerabilidades y la implementación de controles técnicos industriales.	Se enfoca en la implementación de controles técnicos y en la identificación y gestión de riesgos.
Enfoque en riesgos	Utiliza un enfoque basado en riesgos para la gestión de la seguridad de la información, que involucra la identificación de activos críticos de información, la evaluación de riesgos y la implementación de controles adecuados (ISO 27005)	Utiliza un enfoque basado en riesgos, pero se enfoca en la identificación y evaluación de riesgos específicos para los sistemas de control industrial.	Se enfoca en la evaluación y gestión de riesgos, pero está más centrada en la implementación de controles técnicos para mitigar los riesgos identificados.

Controles técnicos	Proporciona un catálogo más amplio de controles técnicos (ISO 27002) y organizativos que pueden ser aplicados a cualquier sistema de información.	Proporciona un marco de referencia detallado para la implementación de controles técnicos específicos para los sistemas de control industrial	Proporciona una lista de controles técnicos recomendados para la protección de los sistemas de control industrial.
Conclusiones de la norma	• Establecimiento de un sistema de gestión de seguridad de la información para la infraestructura de TI • Especifica requisitos genéricos destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. • Describe los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. • La exclusión de cualquiera de los requisitos especificados en estas cláusulas no es aceptable cuando una organización afirma cumplir con este estándar. • Incluye un conjunto de controles que abordan temas de seguridad que deben tenerse en cuenta en una estrategia de seguridad integral en ambientes TI • Se enfoca en el riesgo y permite que una organización pueda seleccionar controles de la lista proporcionada por la norma • Plantea planes de auditoría • Permite tener acceso a la certificación ISO 27001 y cumplir con los requerimientos legales. • Protege la confidencialidad, integridad y disponibilidad de la información en una empresa • Permite investigar los potenciales problemas que podrían afectar la información (evaluación del riesgo) y define lo que es necesario hacer para evitar que los problemas se	• Aborda las necesidades específicas requeridas para la ciberseguridad en entornos TO • Las infraestructuras TO de las instalaciones industriales deben cumplir requisitos específicos de disponibilidad para garantizar la continuidad operativa del sistema • Hace énfasis en que la pérdida de continuidad operativa puede, por ejemplo, manifestarse como una explosión, un apagado abrupto o una fórmula o dosis incorrecta de un elemento que puede poner en riesgo la vida de las personas • Previene condiciones operativas que tendrían consecuencias para la salud, la seguridad y el medio ambiente • Los requisitos de seguridad están diseñados para que no impidan ni interrumpan el funcionamiento seguro • Hace énfasis en la distinción de las implementaciones de control de seguridad de TI y TO • Incluye una lista de controles que abordan aspectos de seguridad en TO que pueden ser complementarios a los controles de la ISO • Describe como las organizaciones deben segmentar su red en zonas y conductos, agrupando sistemas de similar funcionalidad, propósito y/o localización, llevando a cabo un análisis de riesgo y definiendo requerimientos de seguridad por zonas. A cada zona se le asigna un nivel objetivo de seguridad en una escala 1 a 4, dependiente de la	• Aborda la descripción general de los sistemas de control industrial • Propone topologías de sistemas típicos de control industrial • Identifica amenazas y vulnerabilidades típicas en los sistemas de control industrial • Proporciona contramedidas de seguridad recomendadas para la mitigación de los riesgos asociados a los sistemas de control industrial • Gestiona la aplicación de parches de seguridad comparando el entorno TI con el TO • Identifica familias de control de privacidad • El glosario de términos que propone la norma es ampliamente utilizado. • Define los dominios para la gestión de incidentes. • Compila las definiciones de fuentes de amenazas, vulnerabilidades e incidentes contemplando su análisis desde la arquitectura y diseño de los ICS y las redes. • Plantea una arquitectura de defensa en profundidad • Establece reglas generales de los firewalls • Contempla el acceso remoto para soporte • Plantea planes de auditorias • Plantea la identificación de activos críticos para ICS

	produzcan (mitigación o tratamiento del riesgo). • Permite implementar controles bajo la forma de políticas, procedimiento e implementaciones técnicas.	criticidad de la zona para la operación del proceso productivo. • Describe los requerimientos generales de seguridad en términos de identificación y autenticación, confidencialidad de datos, e integridad del sistema, especificando cómo difieren de las redes de ti. En particular, el estándar destaca que la performance y disponibilidad del sistema no deben ser afectadas para cumplir estos requerimientos.	• Brinda recomendaciones para la protección de los sistemas industriales • Se enfoca en la protección de dispositivos y componentes críticos a nivel de fábrica
Niveles pirámide-secciones	• Nivel 1: Manual de seguridad de la información • Nivel 2: Procedimientos • Nivel 3: Instrucciones, checklist y formularios • Nivel 4: Registros	• Nivel 1: general, conceptos y modelos, glosarios. • Nivel 2: políticas y procedimientos • Nivel 3: sistema • Nivel 4: componentes	• Nivel 1: identificar • Nivel 2: proteger • Nivel 3: detectar • Nivel 4: responder • Nivel 5: recuperar

Nota. Análisis de relevancia entre los framewroks identificados Fuente: Elaboración propia.

En la *Tabla* 7 se realizó el análisis de relevancia partiendo de la perspectiva de sistema de gestión de ciberseguridad industrial enfocado a las tecnologías de la operación para mitigar posibles riesgos en las plataformas industriales del sector manufactura-textil. En la *Tabla* 8 se realiza el análisis a nivel de la perspectiva del modelo propuesto en la presente investigación.

Tabla 8. Análisis de relevancia entre los frameworks seleccionados desde la perspectiva del SGCI

Norma / Información	ISO 27001-27002	ISA/IEC 62443	NIST 800-82
Desde la perspectiva del modelo de gestión de ciberseguridad industrial enfocado a las tecnologías de la operación para mitigar posibles riesgos en las plataformas industriales del sector manufactura-textil	• Contempla el contexto de la organización y los fundamentos del negocio. • La gestión del riesgo la plantea en la ISO 27005. • No se identifican las necesidades, la naturaleza tecnológica y el alcance de la ciberseguridad en entornos TO. • La norma está orientada a tecnologías de la información más no se mencionan las tecnologías de la operación. • No se evidencian las consecuencias para la salud, la seguridad y el medio ambiente frente al entorno TO. • Propone la gestión del riesgo desde la ciberseguridad TI. • Si bien, presenta controles que ayudan a mitigar riesgos de ciberseguridad en TI, no especifica cuales de estos se pueden utilizar en TO. • Se requiere un conjunto diferente de estándares, metodologías o normas de la industria para cumplir con las necesidades de seguridad y minimizar los riesgos del ambiente TO. • Modificación de rutinas y procedimientos que encajan muy bien para el ambiente TI pero no para el ambiente TO, no es posible generalizarlos. • Respecto a la delegación de responsabilidades es complejo asignar roles entre las diferentes áreas TI y TO. • Implementarla en su totalidad requiere alta inversión, esfuerzos, dedicación y tiempo. • Menciona controles como la implementación de firewalls, antivirus	• Contempla el contexto de la organización y los fundamentos del negocio. • Cuenta con un apéndice de gestión del riesgo. • Centrado en la mitigación de vulnerabilidades en infraestructuras críticas para los sectores industriales oil, gas y nuclear. • Se enfoca en la fabricación de tecnología industrial y prestación de servicios esenciales. • Propone la gestión del riesgo desde la ciberseguridad industrial. • No se ocupa de la seguridad de la información. • Propone generar la estrategia de ciberseguridad industrial. • No propone el establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. • Propone arquitecturas segmentadas de redes con capas de protección. • Propone la segmentación de redes a través del modelo de Pardue. • No especifica el versionamiento de los desarrollos. • No involucra auditores y organismos de certificación.	• Si bien propone la segmentación de la red e implementación de firewall, no especifica los puntos de protección ni la definición de zonas y conductos entre los dispositivos TO. • No propone el establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información. • Identifica la selección de los activos industriales críticos. • No aborda las necesidades específicas para la ciberseguridad en entornos TO. • No involucra organismos de certificación. • Propone la cultura de seguridad. • Establece el framework de ciberseguridad bajo sus pilares: Identificar, proteger, detectar, responder y recuperar. • Establece la continuidad y resiliencia del negocio a nivel industrial. • Integra la definición de la política de ciberseguridad industrial a través de sus pilares de referencia.

	pero no se especifica que los ambientes TO no trabajan con los mismos protocolos de TI y los antivirus bloquean los procesos del software. • No propone la defensa multinivel basada en zonas y conductos. • Proporciona 14 categorías de control con 114 controles los cuales no todos aplican a TO. • No contiene medidas de seguridad para sistemas de control • No contempla los requerimientos de seguridad en la adquisición de dispositivos. • No contempla impactos físicos potenciales de un incidente de seguridad en entornos TO • Menciona la segmentación de redes pero a nivel de VLANs para el ambiente TI. • Propone la promoción de la cultura en seguridad de la información.	• No sugiere políticas generales en los cortafuegos. • Contempla la defensa en profundidad basándose en la ISA95 y el modelo de Pardue. • Propone la promoción de la cultura en ciberseguridad industrial.	

Nota. Análisis de relevancia entre los frameworks seleccionados desde la perspectiva del SGCI Fuente: Elaboración propia.

Como se evidencia en la *Tabla* 8, no se encontró un marco específico a nivel industrial que genere un modelo de ciberseguridad industrial, por el contrario, la variedad de enfoques presentados en cada uno de los marcos de referencia enriquece el proceso de selección de las mejores prácticas para la construcción del modelo propuesto en este proyecto. Este análisis de relevancia ha permitido identificar y fusionar elementos sobresalientes de cada marco, creando así un modelo sólido y completo que se adapta de manera óptima a las necesidades específicas de las organizaciones del sector manufactura-textil.

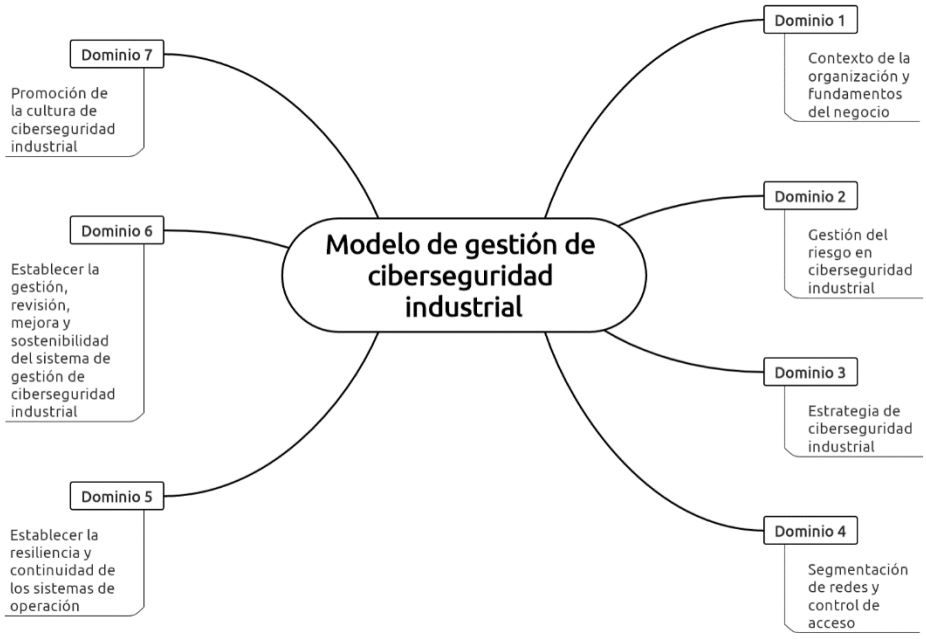
FASE II - CONSTRUCCIÓN DEL SISTEMA DE GESTIÓN DE CIBERSEGURIDAD INDUSTRIAL.

La creación de un modelo de ciberseguridad industrial es fundamental para salvaguardar los sistemas de control y automatización empleados en los procesos industriales del sector manufactura-textil. Estos sistemas pueden resultar vulnerables a ataques cibernéticos que podrían tener consecuencias graves, como la interrupción de la producción, la pérdida de datos, el deterioro de los equipos y la eventual exposición de información confidencial. Por lo anterior, y teniendo como referencia el análisis de relevancia realizado en las *Tablas* 7 y 8, se propone el desarrollo del segundo objetivo específico "Construir un sistema de gestión de ciberseguridad industrial enfocado en las TO del sector manufactura-textil soportado por las mejores prácticas de los marcos de ciberseguridad".

Construcción del sistema de gestión de ciberseguridad industrial

La construcción de un sistema de ciberseguridad en el ámbito de la manufactura-textil se convierte en un pilar fundamental para la protección de los activos críticos y la mitigación de los riesgos inherentes a los ataques cibernéticos. En dicho sector, los sistemas de control y automatización industrial, están diseñados para operar en un entorno confiable y seguro. Un sistema robusto de ciberseguridad industrial es esencial para asegurar que estas plataformas continúen operando correctamente, preservando así la disponibilidad, integridad y confidencialidad. Como se aprecia en la *Figura* 6, se crearon los siete dominios más relevantes para la construcción del sistema de gestión de ciberseguridad industrial para el sector manufactura-textil basados en las mejores prácticas de los marcos de referencia investigados, estos dominios permiten mitigar la materialización de riesgos en el ámbito industrial en este tipo de organizaciones.

Figura 6. Dominios del modelo de gestión de ciberseguridad industrial



Nota. Dominios del sistema de gestión de ciberseguridad industrial para el sector manufactura textil Fuente: Elaboración propia

DOMINIO 1: CONTEXTO DE LA ORGANIZACIÓN Y FUNDAMENTOS DEL NEGOCIO.

En el contexto de la industria manufactura-textil, este ámbito se revela como uno de los pilares más importantes al iniciar la construcción del SGCI. El objetivo principal es comprender el entorno organizacional y los fundamentos del negocio con el fin de identificar las necesidades específicas en términos de ciberseguridad. Estas necesidades deben abordar una amplia gama de aspectos, incluyendo los procesos de negocios, los aspectos industriales, financieros, la salud laboral y seguridad física, los aspectos medioambientales y, en general, cualquier elemento que pueda impactar en el correcto funcionamiento de los procesos de negocios de la organización.

Los fundamentos del negocio deben destacar de manera clara la dependencia que tiene la organización de sus sistemas de control, subrayando así la necesidad de garantizar tanto su seguridad física como lógica. Esto, a su vez, puede servir como una herramienta de persuasión interna para obtener el apoyo de la dirección de la organización en la creación y desarrollo del SGCI, reconociendo su relevancia en la preservación de la operatividad y competitividad de la industria textil.

Dado lo anterior, se generó la plantilla “Anexo 01 - Dominio 1 - Contexto de la organización”. En este documento se abordan los siguientes escenarios los cuales deben ser diligenciados por la empresa del sector manufactura-textil para la implementación el SGCI:

- Propósito, alcance y audiencia objetivo.
- Fundamentos del negocio.
- Beneficios de la implementación del SGCI.
- Estimación de esfuerzos necesarios para la implementación del SGCI.

DOMINIO 2: GESTIÓN DEL RIESGO EN CIBERSEGURIDAD INDUSTRIAL.

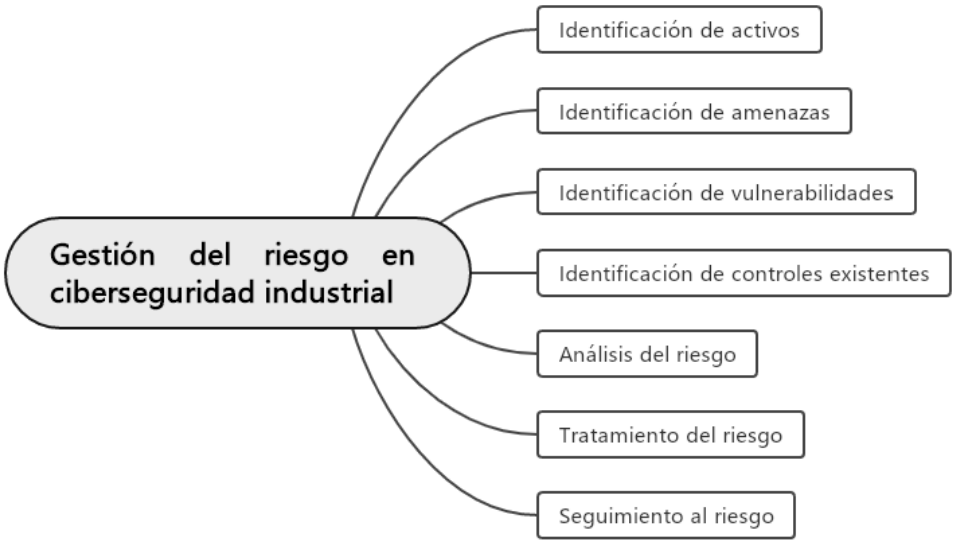
Este dominio permite identificar y evaluar las amenazas cibernéticas que pueden afectar las instalaciones industriales del sector manufactura-textil, también permite estimar el posible impacto y la probabilidad de la materialización de los riesgos. Existen diferentes metodologías de análisis de riesgos, algunas de las cuales son aplicables en los entornos de sistemas de control. En este dominio, el objetivo es explicar los componentes esenciales de una metodología adecuada para analizar riesgos en estos entornos con el fin de poderlos validar en la fase III del presente proyecto.

En el análisis de riesgos, se pueden utilizar dos enfoques distintos basados en cómo se caracteriza el riesgo, uno de ellos es el análisis cuantitativo y el otro el análisis cualitativo. El primero, busca valorar el riesgo en términos numéricos, generalmente en forma de pérdidas financieras. Aunque estos resultados son comprensibles desde la perspectiva empresarial y organizativa, obtenerlos con precisión es complejo en el sector manufactura-textil, esto se debe a que dependen de la correcta evaluación de las probabilidades de ocurrencia de amenazas y vulnerabilidades, así como del impacto causado por la pérdida o el deterioro de los activos críticos. El segundo, se basa en el conocimiento y la experiencia de expertos y especialistas, tanto internos como externos, así como en la opinión de los usuarios de los activos críticos afectados. Este enfoque emplea niveles de probabilidad y severidad que se aplican a los distintos elementos del análisis, como los activos, las amenazas y las vulnerabilidades.

En la presente metodología, se ha decidido adoptar un enfoque cualitativo para el análisis de riesgos en entornos industriales. Esta elección se fundamenta en la falta de recursos que permitan obtener valores históricos precisos sobre amenazas, vulnerabilidades e impactos en este contexto. El enfoque cualitativo resulta más adecuado debido a su capacidad para considerar el conocimiento de expertos y la experiencia acumulada en lugar de depender únicamente de datos cuantitativos que podrían ser difíciles de recopilar.

En la *Figura* 7, se proponen las fases metodológicas del modelo para la ejecución del dominio 2 correspondiente a la gestión del riesgo en ciberseguridad industrial, abordaremos cada una de las fases.

Figura 7. Pilares de la gestión del riesgo en ciberseguridad industrial



Nota. Gestión del riesgo en ciberseguridad industrial Fuente: Elaboración propia

- **Identificación de activos:**

La identificación de activos es el primer paso para la ejecución del análisis de riesgos. Aquí se debe realizar el inventario de los activos industriales que se encuentran dentro del alcance del análisis. Es importante indicar que esté ejercicio constituye la base para un análisis de riesgos el cual debe estar definido de manera correcta debido a que realizar una identificación minuciosa de los activos posibilitará una comprensión en profundidad de las posibles vulnerabilidades y amenazas a las que la organización podría estar expuesta. A partir de este conocimiento, será factible proceder con una evaluación precisa de los riesgos y la introducción de medidas adecuadas para reducirlos.

Para el proceso de identificación de activos, se propone la *Tabla* 9, esta deberá ser diligenciada en conjunto con la empresa del sector textil.

Tabla 9. Estructura del inventario de activos industriales

INVENTARIO						VALORACIÓN				
Nombre de activo	**Descripción del activo**	**Sistema involucrado**	**Tipo de activo**	**Tipo de ubicación**	**Propietario del activo**	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Valor**	**Nivel de tasación**

Nota. Estructura del inventario de activos industriales Fuente: Elaboración propia

Para mayor entendimiento, a continuación se explica cada uno de los campos de la estructura:

- Nombre del activo: Nombre del elemento que le genera valor a la organización.
- Descripción del activo: Descripción de la función principal del activo.
- Sistema involucrado: Sistema industrial del cual hace parte el activo.
- Tipo de activo: Especificar el tipo de activo (información, software, físico, intangible, personas, servicios).
- Tipo de ubicación: Indicar si el activo es físico, lógico.
- Propietario del activo: Especificar quien es el dueño o propietario del activo.
- Valoración: Este campo se determina de acuerdo al criterio de la *Tabla* 10, correspondiente a la disponibilidad del activo.

Tabla 10. Valor del activo con base a su disponibilidad

VALOR DEL ACTIVO	DISPONIBILIDAD
5 (Muy Alto)	Se requiere que el activo nunca se encuentre indisponible, pues su carencia afectaría irreversiblemente a la organización.
4 (Alto)	Se considera que como máximo el activo puede estar indisponible por una hora, pues su carencia afectaría gravemente a la organización.
3 (Medio)	Se considera que como máximo el activo puede estar indisponible por un día, pues su carencia afectaría considerablemente a la organización.
2 (Bajo)	Se considera que como máximo el activo puede estar indisponible por una semana, pues su carencia afectaría parcialmente a la organización.
1 (Muy Bajo)	Se considera que como máximo el activo puede estar indisponible por tiempo indefinido, pues su carencia no impacta a la organización.

Nota. Valor del activo con base a su disponibilidad Fuente: Elaboración propia

- Valor del activo y nivel de tasación: Se estima el valor del activo del promedio de sumar los valores del nivel de importancia respecto a la triada de la ciberseguridad (disponibilidad, integridad y confidencialidad) y se le asocia el nivel de tasación según la distribución de la *Tabla* 11.

Tabla 11. Valor del activo y nivel de tasación

Valor del Activo	Nivel de Tasación
4.001 – 5.000	Muy Alto
3.001 – 4.000	Alto
2.001 – 3.000	Medio
1.001 – 2.000	Bajo
0.000 – 1.000	Muy Bajo

Nota. Valor del activo y nivel de tasación Fuente: Elaboración propia

Para la identificación de los activos industriales, se construyó la plantilla de inventario de activos industriales, "Anexo 02 – Dominio 2 - Inventario de activos industriales". Este documento se debe diligenciar en conjunto con la organización.

- **Identificación de amenazas**

Las amenazas presentan la capacidad de causar daño a elementos como la información, los procesos y los sistemas. Esto, a su vez, puede interferir con la correcta ejecución de los procedimientos de producción de la organización. Dichas amenazas pueden originarse de manera intencionada (deliberadas) o de forma no intencional (accidentales). Estas amenazas pueden provenir tanto de entornos externos como dentro de la propia organización, y pueden manifestarse en diversas formas. Indiferentemente de estas circunstancias, es crucial reconocer las amenazas que pueden impactar a los activos críticos identificados en la etapa anterior.

Identificar estas amenazas y evaluar su probabilidad de ocurrencia demanda la experiencia y el conocimiento proporcionado por el experto en las plataformas industriales. Esto incluye los responsables de los elementos afectados, los usuarios, el personal encargado de su mantenimiento, especialistas en ciberseguridad, y profesionales o entidades con pericia para ofrecer opiniones informadas en esta materia y en el sector.

Para la identificación de las amenazas en ambientes industriales, se construyó la plantilla de identificación de amenazas, "Anexo 03 – Dominio 2 - Inventario de amenazas". Este documento se debe diligenciar en conjunto con la organización.

- **Identificación de vulnerabilidades**

Las vulnerabilidades representan áreas frágiles en los activos críticos. La existencia de una vulnerabilidad por sí sola no tiene un efecto perjudicial, ya que se necesita una amenaza para aprovecharla. Aquellas vulnerabilidades que no cuenten con amenazas asociadas no exigirán la implementación de controles adicionales. No obstante, es necesario documentarlas y mantener un seguimiento para identificar cualquier cambio que se presente. Las vulnerabilidades se clasifican en distintos tipos y, para cada una, se proponen amenazas específicas capaces de explotar dicha vulnerabilidad. La clasificación basada en los tipos de vulnerabilidades facilita de manera práctica la asignación de grupos de vulnerabilidades a categorías de activos. Este enfoque simplifica el proceso de identificación y asignación de medidas de seguridad a los diferentes elementos.

Para la identificación de las vulnerabilidades en ambientes industriales, se construyó la plantilla de identificación de vulnerabilidades, "Anexo 04 – Dominio 2 - Inventario de vulnerabilidades. Este documento se debe diligenciar en conjunto con la organización.

- **Identificación de controles existentes**

Es esencial realizar la identificación de los controles que se tienen implementados, esto con el fin de evitar gastos y esfuerzos innecesarios. En este proceso de identificación, se lleva a cabo la verificación del funcionamiento apropiado de los controles previamente implementados por la organización. Además, se evalúa si estos mismos controles están introduciendo nuevas vulnerabilidades en el ámbito contemplado. Para descubrir los controles existentes, es posible aprovechar diversas fuentes de información al interior de la organización como:

- Documentación que detalla los controles, como los planes de manejo de riesgos.
- Documentos internos de gestión, tales como protocolos para la entrada y salida de personal.
- Registros generados por los sistemas.
- Históricos de supervisión.
- Individuos encargados de la seguridad o de la operación y supervisión de los elementos dentro del ámbito.
- Evaluaciones directas en el lugar de trabajo para los controles físicos vigentes.
- Resultados de auditorías.

La identificación de estos controles previos es crucial para garantizar que no se dupliquen esfuerzos ni recursos, al mismo tiempo se asegura el correcto funcionamiento y la eficacia general de las medidas de seguridad implementadas.

Para la identificación de los controles existentes en el ambiente industrial, se construyó la plantilla de identificación de controles, "Anexo 05 – Dominio 2 - Inventario de controles existentes". Este documento se debe diligenciar en conjunto con la organización.

- **Análisis del riesgo**

El riesgo se refiere a un valor resultante de la combinación entre el impacto potencial (consecuencias) que podría derivar de la degradación o pérdida de un activo (o conjunto de activos), y la probabilidad de que una vulnerabilidad presente en el activo sea aprovechada por una amenaza interna o externa. Este riesgo se calcula mediante la fórmula: Riesgo = Probabilidad x Impacto

En el enfoque cualitativo seleccionado, la probabilidad de que una vulnerabilidad sea explotada por una amenaza generando un impacto para la organización puede representarse mediante una matriz 5x5 tomando como referencia el modelo del estándar IEC62443.

Para el cálculo del riesgo en el ambiente industrial se construyó la plantilla de cálculo del riesgo, "Anexo 06 - Dominio 2 - Gestión de riesgo". Este documento se debe trabajar en conjunto con la organización para determinar los riesgos que a hoy tiene la empresa. En cada una de las hojas del documento, se debe diligenciar la información que se ha venido trabajando previamente.

- **Tratamiento del riesgo**

Lograr una eliminación total del riesgo en los entornos industriales resulta prácticamente inviable. Esto se debe a la intrincada naturaleza de estos ambientes, donde las amenazas y vulnerabilidades siempre persistirán, con la posibilidad de afectar la operación de los procesos industriales. En consecuencia, abordar el tratamiento del riesgo exige identificar las amenazas prioritarias que deben ser abordadas con el objetivo de reducirlas a niveles aceptables. Esta elección de riesgos prioritarios se basa en aquellos que poseen un mayor grado de peligro, aunque también se considerarán aquellos que pueden ser tratados con soluciones inmediatas. Esta estrategia se fundamenta en que la reducción de estos riesgos contribuye a evidenciar los logros del sistema de gestión de seguridad industrial y a difundir sus resultados dentro de la organización.

La decisión de qué contramedidas implementar se realiza considerando un equilibrio entre el costo, el beneficio y la operatividad. En los contextos industriales, es crucial asegurarse de que la implementación de una contramedida no perturbe la disponibilidad y la operación de los sistemas en uso.

Las contramedidas pueden ser distintas, desde la introducción de nuevos dispositivos hasta modificaciones en la configuración, la creación y aplicación de procedimientos, y cualquier otra modificación en la infraestructura que contribuya a la reducción del riesgo.

Para el tratamiento de los riesgos se debe generar la matriz de riesgos enfocada en los tres pilares de la seguridad informática (disponibilidad, confidencialidad e integridad) que permita tener un panorama de los tratamientos de los riesgos. Este apartado se debe documentar en el “Anexo 06 - Dominio 2 - Gestión de riesgo” específicamente en la hoja de tratamiento.

- **Seguimiento al riesgo**

El seguimiento al riesgo en ciberseguridad industrial es una fase crítica dentro del proceso de gestión de riesgos. Implica una supervisión constante de las amenazas y vulnerabilidades que enfrenta una infraestructura industrial, así como la efectividad de las medidas de mitigación implementadas. Esto incluye la recopilación de datos en tiempo real, la monitorización de eventos de seguridad, la revisión periódica de políticas y procedimientos, y la adaptación a las nuevas amenazas emergentes. El seguimiento al riesgo no solo busca identificar y evaluar nuevas amenazas, sino también garantizar que las estrategias de seguridad sean dinámicas y puedan ajustarse rápidamente para mantenerse al día con el cambiante panorama de la ciberseguridad industrial. Es una parte esencial para proteger los activos críticos y garantizar la continuidad de las operaciones en entornos industriales altamente conectados y digitalizados. Con esta fase se garantiza que la gestión de riesgos sean un ciclo PHVA que continuamente esté madurando respecto de las lecciones aprendidas. Este apartado se debe documentar en el “Anexo 06 - Dominio 2 - Gestión de riesgo” específicamente en la hoja de tratamiento en el plan de monitoreo.

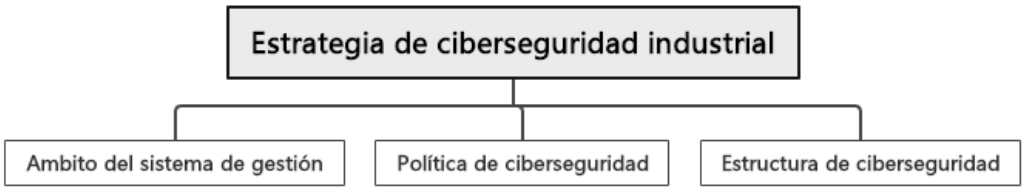
Para el desarrollo del dominio 2, correspondiente a la gestión del riesgo, se construye el “Anexo 06 - Dominio 2 - Gestión de riesgo”.

DOMINIO 3: ESTRATEGIA DE CIBERSEGURIDAD INDUSTRIAL.

La estrategia de ciberseguridad es un enfoque integral y planificado que la organización adopta para gestionar y mitigar los riesgos asociados con las amenazas cibernéticas y la seguridad de la información. Esta estrategia abarca un conjunto de acciones, políticas, procedimientos y medidas diseñadas para proteger los activos de información, mantener la disponibilidad, integridad y confidencialidad de los datos, y garantizar el funcionamiento ininterrumpido de los sistemas y servicios digitales.

La estrategia de ciberseguridad se apoya en los fundamentos del negocio del anexo 01 – Dominio 1 – Contexto de la organización, donde se identifica la estrategia de la compañía y sus necesidades, partiendo de esto se propone la *Figura* 8, correspondiente a la creación de los tres pilares fundamentales para la estrategia de ciberseguridad industrial.

Figura 8. Estrategia de ciberseguridad industrial



Nota. Diagrama con la estrategia de ciberseguridad industrial para el sector manufactura-textil Fuente: Elaboración propia

A continuación, se amplía la información respecto a cada uno de los pilares de la estrategia de ciberseguridad industrial propuesta para el SGCI:

- Ámbito del Sistema de Gestión de Ciberseguridad Industrial (SGCI):

Se delimita el alcance del SGCI de acuerdo a los requisitos empresariales definidos en los fundamentos del negocio.

- Política de Ciberseguridad Industrial:

Se formalizan los requerimientos de seguridad que deben implementarse dentro del alcance establecido, impulsándolos en toda la entidad y designando responsabilidades generales para su cumplimiento.

La política de ciberseguridad tiene como objetivo principal proporcionar directrices con respecto a la administración y respaldo de la ciberseguridad. Estas directrices deben estar en línea tanto con los requerimientos empresariales como con las regulaciones legales aplicables. La Política de Ciberseguridad cumple varias funciones esenciales, entre ellas:

  - Reflejar la intención de la alta dirección: Esta política materializa la postura de la dirección en relación a la ciberseguridad industrial.
  - Ofrecer soporte y direccionar la estrategia: La dirección debe proporcionar respaldo y orientación a través de la política para la implementación de medidas de ciberseguridad industrial en armonía con los requerimientos comerciales y el cumplimiento normativo.

- Mejorar la concientización: Se busca reforzar la comprensión dentro de la organización sobre la importancia de la ciberseguridad industrial.
- La política de ciberseguridad debe estar avalada por la alta dirección, esto demuestra su apoyo y compromiso con la organización.

Respecto al contenido de la estrategia, se recomienda que la política contenga la mayoría de los siguientes puntos:

- Una definición de ciberseguridad, sus objetivos y alcance.
- El respaldo explícito de los responsables de los procesos empresariales a proteger.
- La definición de responsabilidades generales y específicas sobre ciberseguridad industrial, incluyendo la comunicación de incidentes de seguridad.
- Mención de los métodos en uso para identificar y gestionar el riesgo.
- Alusiones a la documentación respaldatoria de la política, como políticas adicionales, procedimientos, y guías operativas.
- Implementación de revisiones para asegurar la vigencia de la ciberseguridad a lo largo del tiempo.
- Principales requerimientos de la organización, tales como el cumplimiento de leyes, regulaciones y contratos, formación y capacitación en seguridad, continuidad de negocio, y las consecuencias de violar la Política de Ciberseguridad.
- La política de ciberseguridad debe estar acompañada por sanciones para el personal que la incumpla.

La política se debe revisar de manera periódica para asegurar su vigencia en el tiempo. Esta política es la base de entrada al SGCI y de ella se pueden derivar otros documentos más específicos. La política proporciona una vista general de alto nivel sobre la ciberseguridad dentro de la organización, evitando detalles técnicos u operativos. Los detalles específicos de ciberseguridad para distintos componentes se detallarán en documentos subordinados a la política.

- Estructura de Ciberseguridad:

Es esencial establecer el área encargada de gestionar y mantener la ciberseguridad de los sistemas de control industrial dentro de la organización. La ciberseguridad abarca no solo los sistemas en sí y la información que manejan, sino también otros elementos vinculados a los activos que se buscan proteger. En este sentido, se deben considerar aspectos de seguridad física, proveedores, terceras partes, asociados y socios. El compromiso de la organización con el SGCI desempeña un papel crucial para el éxito de esta iniciativa y debe ser liderado por un grupo de personas expertas en el tema. Este compromiso debe arraigarse desde los niveles más altos de la jerarquía, ya que requiere la contribución de conocimiento en toda la organización y posiblemente llevará a ajustes en su estructura.

La alta dirección es la responsable de instaurar una estructura organizativa que no solo ofrezca orientación y supervisión para la administración de la ciberseguridad de los sistemas de control, sino que también provea los recursos necesarios para llevar a cabo las tareas relacionadas con el mantenimiento y operación del SGCI.

Esta estructura puede adoptar la forma de un grupo de interés o un comité de gestión de ciberseguridad. Este grupo debe poseer el conocimiento esencial para implantar y operar el SGCI, asumiendo las responsabilidades relevantes en ciberseguridad y rindiendo cuentas directamente ante la alta dirección. El comité debe estar conformado por empleados relevantes de diversas áreas de la organización que cuenten con experiencia o responsabilidades en relación con la ciberseguridad de los sistemas de control de la compañía. En caso de ser necesario, el comité puede ser complementado de manera permanente o temporal con expertos externos especializados en áreas particulares. La composición del comité puede variar a lo largo del tiempo para adaptarse a la evolución de los sistemas organizativos y al aumento en la madurez de la organización en lo que respecta a la ciberseguridad de los sistemas de control.

Este comité de gestión en ciberseguridad tendrá la tarea de coordinar la implementación y operación del SGCI. Además, tomará decisiones en relación con la ciberseguridad que afecten a los sistemas de control de la organización. La coordinación del comité será responsabilidad de un líder designado por la alta dirección, cuyas funciones incluirán organizar las reuniones del comité y supervisar el funcionamiento del SGCI en última instancia. Un componente fundamental de esta estructura organizativa de ciberseguridad implica la asignación de responsabilidades de ciberseguridad en diversos niveles de la organización.

Es igualmente esencial fomentar la integración de los roles de seguridad derivados del SGCI con otras iniciativas organizativas (principalmente en comités ya activos en la entidad). Este enfoque tiene como objetivo maximizar las sinergias organizativas en la mayor medida posible.

Los pilares propuestos en la *Figura* 8, son esenciales para construir una estrategia de ciberseguridad sólida y efectiva. Cada uno de ellos desempeña un papel fundamental en la creación de una base que garantice la protección de los activos de información y la mitigación de riesgos en línea con los objetivos y necesidades de la organización. Para la estrategia de Ciberseguridad industrial se construyó el “Anexo 07 - Dominio 3 - Estrategia de ciberseguridad industrial”, en este documento se define el ámbito del SGCI, la política de ciberseguridad industrial y la estructura de ciberseguridad que definirá la organización donde se implemente el SGCI.

DOMINIO 4: SEGMENTACIÓN DE REDES Y CONTROL DE ACCESO.

En este dominio se propone la construcción de la arquitectura de segmentación física y lógica de los ambientes TO. Para mitigar los riesgos de ciberseguridad se deben definir los niveles, zonas y conductos apoyados bajo el modelo PERA (Purdue Enterprise Reference Architecture) referenciado en el estándar ISA-95.

El Modelo de Purdue es un enfoque de segmentación de redes industriales contenido en las buenas prácticas del estándar la ISA95, es utilizado para organizar y proteger sistemas en entornos industriales críticos, como plantas de fabricación y control de procesos. Apoyados de este modelo, se divide la red en cuatro niveles jerárquicos que representan diferentes capas de la infraestructura y la automatización industrial para el ambiente manufactura-textil.

- Nivel 0 - Proceso: En este nivel, se encuentran los dispositivos y sensores que interactúan directamente con el proceso industrial, como sensores de temperatura, válvulas y actuadores. Estos dispositivos suelen estar conectados a un controlador lógico programable (PLC).
- Nivel 1 - Control: En este nivel, se encuentran los controladores lógicos programables (PLC) y las unidades de control distribuido (DCS). Estos sistemas supervisan y controlan los procesos industriales y recopilan datos de los dispositivos del nivel 0.
- Nivel 2 - Supervisión: Aquí se ubican las estaciones de supervisión y control, que proporcionan una interfaz de usuario para supervisar y controlar los procesos industriales. Los sistemas SCADA (Supervisory Control and Data Acquisition) son comunes en este nivel.
- Nivel 3- Gestión de la Planta: En este nivel, se lleva a cabo la gestión de la planta y la planificación de la producción. Los sistemas de ejecución de fabricación (MES) suelen utilizarse para coordinar la producción.
- Nivel 4 - Empresarial: El nivel más alto del modelo es el nivel de la empresa, donde se encuentran las aplicaciones y sistemas empresariales que gestionan la planificación, la logística, la gestión de pedidos y otras funciones empresariales.

Para dar claridad a los niveles respecto a la segmentación de las redes, en la presente investigación se basa en la pirámide anteriormente propuesta en el modelo PERA de la *Figura* 5, mencionada en el estándar ISA95. Los niveles expuestos en la *Figura* 5 deberán ser identificados en la organización para trazar la ruta de la segmentación de redes, adicionalmente, se propone que estén acompañados por la implementación de una política de control de acceso que permita mitigar los riesgos en los ambientes industriales validando que los accesos a la infraestructura crítica sean los correctos. En la *Figura* 9, se proponen las fases del control de acceso del sector manufactura-textil.

Figura 9. Control de acceso

Nota. Componentes del control de acceso TO Fuente: Elaboración propia

A continuación, se amplía la información de cada uno de los pilares que integran el control de acceso propuesto.

- **Identificación:**

Es el primer paso en el proceso propuesto. El proceso de identificación implica que un usuario se presente ante el sistema y afirme su identidad. Esto generalmente se logra mediante un nombre de usuario o identificador único y una contraseña o algún otro método de autenticación, como una tarjeta de acceso,

huella dactilar o autenticación biométrica. La identificación es la acción de informar al sistema quién eres. El proceso de identificación permite al sistema reconocer al usuario y determinar si debe o no brindar el acceso.

- **Autenticación:**

Es el proceso de verificar la identidad de un usuario que intenta acceder a un sistema informático o a una aplicación. Es la segunda fase del proceso de control de acceso y tiene como objetivo asegurarse de que la persona o entidad que se presenta ante el sistema es quien afirma ser. La autenticación se basa en la idea de que, además de proporcionar una identificación (nombre de usuario o identificador único), el usuario debe demostrar que es legítimo utilizando un factor de autenticación. Estos factores pueden ser:

  - Conocimiento: Algo que el usuario conoce, como una contraseña, un PIN o una respuesta a una pregunta de seguridad.
  - Poseer: Algo que el usuario posee, como una tarjeta de acceso, un teléfono móvil o un token de seguridad que genera códigos temporales.
  - Biometría: Algo que el usuario es, como una huella dactilar, un escaneo de retina, una voz o una cara reconocible.

La autenticación combina la identificación (quién eres) con la verificación de que realmente eres quien afirmas ser mediante uno o más de estos factores de autenticación. El objetivo es garantizar que nadie más que el usuario autorizado pueda acceder al sistema o a los recursos protegidos.

Los sistemas informáticos suelen requerir uno o más factores de autenticación para reforzar la seguridad. Por ejemplo, al acceder a un sistema SCADA, la plataforma debe solicitarle al usuario su nombre de usuario (identificación) y contraseña (factor de conocimiento). En la autenticación de dos factores (2FA), se agrega un segundo factor, como un código generado por una aplicación de autenticación en el teléfono del usuario.

La autenticación robusta es esencial para proteger la privacidad y la seguridad de los datos, especialmente en entornos críticos como los industriales. Al combinar la identificación con factores de autenticación, se dificulta que los atacantes accedan a cuentas y datos sin autorización.

- **Autorización:**

Una vez que un usuario ha demostrado su identidad a través del proceso de autenticación, la fase de autorización determina qué recursos o acciones específicas tiene permiso para realizar dentro del sistema, es decir, la autorización se encarga de responder a la pregunta: “Después de haber verificado quién es el usuario, ¿qué puede hacer ese usuario en el sistema?". Esta fase define los derechos y privilegios del usuario en función de su identidad y su contexto dentro del sistema.

Las decisiones de autorización se basan en políticas de seguridad previamente definidas. Estas políticas establecen las reglas y restricciones que determinan quién tiene acceso a qué recursos y bajo qué condiciones. La política de autorización debe incluir:

  - Roles y permisos: Se deben definir los roles de los usuarios en los sistemas por ejemplo especificar si es un usuario, administrador o empleado, posterior a esta definición se deben asignar los permisos a los recursos que pueden realizar o acceder los usuarios en función de su rol. Por ejemplo, un

empleado puede tener permiso para ver información de la planta de producción, mientras que un administrador puede tener permiso para realizar cambios en la configuración del sistema SCADA.
- Grupos: Los usuarios deben agruparse en categorías o grupos, y las políticas de autorización se aplican a grupos enteros en lugar de usuarios individuales con el fin de minimizar la administración. Esto simplifica agrupar correctamente los usuarios y realizar procedimientos de depuración.
- Contexto: La autorización puede tener en cuenta factores contextuales, como la hora del día, la ubicación geográfica o el dispositivo desde el cual se está accediendo. Por ejemplo, un sistema industrial puede permitir el acceso a ciertos recursos solo durante el horario laboral. Este control es importante para garantizar que los sistemas sean accedidos bajo las políticas definidas por la organización.
- Niveles de confidencialidad y clasificación de datos: Se recomienda clasificar los datos en función de su nivel de confidencialidad y aplicar políticas de autorización. Esto con el fin de que los usuarios solo pueden acceder a datos que estén clasificados dentro de su nivel de autorización.

- **Trazabilidad:**

Esta fase se enfoca en registrar y rastrear todas las actividades relacionadas con el acceso y el uso de los recursos del sistema por parte de los usuarios. La trazabilidad es esencial para la seguridad cibernética y la conformidad con regulaciones y estándares de seguridad. Se propone una etapa de registro de eventos donde se aloje la información relevante frente al inicio de sesión, intentos fallidos de acceso, cambios de permisos de usuario, acceso a información sensible. Adicionalmente se propone una auditoría y seguimiento, esto con el fin de supervisar las actividades del usuario para detectar cualquier comportamiento sospechoso o actividades no autorizadas.

La política de control de acceso permite proteger los recursos y la información crítica de la organización, prevenir amenazas tanto internas como externas, garantizar el cumplimiento normativo y mantener la integridad de los sistemas y datos.

DOMINIO 5: ESTABLECER LA RESILIENCIA Y CONTINUIDAD DE LOS SISTEMAS DE OPERACIÓN.

En este dominio se establecen los componentes de resiliencia y continuidad de los sistemas de operación, se define el alcance, las políticas, los objetivos, los responsables y los diferentes comités que permitirán garantizar esta fase. Adicionalmente se establece el impacto en tecnologías de la operación y se definen los procedimientos de resiliencia y continuidad de la operación.

- **Alcance y política en el sector manufactura textil**

Para asegurar la resiliencia y la continuidad de los sistemas de operación y control en el sector manufactura textil, es esencial adoptar un enfoque integral y holístico que permita implementar un conjunto de capacidades destinadas a la protección constante de las operaciones de la organización. Estas capacidades deben centrarse principalmente en las infraestructuras y otros recursos críticos que respaldan el proceso de

producción textil. Además, es importante tener en cuenta que, en ciertas jurisdicciones, la legislación define los servicios esenciales dentro de sectores estratégicos. Las empresas textiles, al formar parte de los sectores estratégicos del país, deben poseer la capacidad de mantener la resiliencia cibernética frente a diversos ataques, amenazas e incidentes que puedan presentar.

Para respaldar la estrategia de resiliencia y continuidad, es fundamental contar con una política claramente definida, junto con sus respectivas normas y procedimientos de implementación. Un conjunto documentado de estas políticas es crucial para alinear las actividades de resiliencia con la misión de la organización, establecer expectativas precisas, crear las condiciones necesarias para la mejora continua del sistema, ofrecer orientación sobre las necesidades operativas, mantener la consistencia, confiabilidad y continuidad en las operaciones de producción.

La ausencia de una política adecuada puede obstaculizar la capacidad de gestionar la resiliencia y la continuidad en la manufactura textil.

La política de resiliencia y continuidad debe incluir la declaración de su propósito, alcance y audiencia objetivo en caso de incidentes cibernéticos que afecten los sistemas de operación y control industrial en la organización. Además, esta política debe contener una clara asignación de responsabilidades y apoyarse en la estructura organizativa previamente realizada la cual debe garantizar la implementación de medidas adecuadas para lograr la resiliencia de los procesos industriales en la empresa frente a ciber-incidentes. Estas medidas deben ser compatibles con las capacidades de continuidad del negocio y de respuesta a incidentes de la empresa del sector manufactura textil.

- **Objetivos y métricas para la resiliencia en el sector manufactura textil**

El propósito fundamental de un enfoque orientado a la resiliencia en una empresa del sector manufactura textil es forjar una visión compartida y colectiva de la capacidad de la organización para enfrentar los riesgos que puedan impactar negativamente en la operación normal de sus servicios críticos, incluso llegando a situaciones de crisis.

Uno de los principios esenciales para lograr la resiliencia es reconocer que una organización moviliza sus activos, incluyendo personal, información, tecnología e instalaciones, para cumplir su misión específica, como, por ejemplo, la producción y suministro de servicios críticos para la sociedad. Siguiendo este principio, se pueden identificar las necesidades de la organización para planificar, definir, desarrollar, gestionar y evaluar las prácticas y comportamientos necesarios que conduzcan a la resiliencia corporativa en el ámbito de la manufactura textil.

Las métricas, medidas e indicadores utilizados en la gestión de incidentes son los criterios fundamentales para evaluar la efectividad y eficiencia de la función de gestión de incidentes. Las métricas basadas en Indicadores Clave de Desempeño (KPI) y los objetivos del programa establecidos para la gestión de incidentes deben presentarse ante la alta dirección como una base sólida para justificar la continua inversión y funcionamiento de estas prácticas. Estos indicadores permiten a la alta dirección comprender la capacidad de gestión de incidentes de la organización y las áreas de riesgo que requieren atención especial.

Las medidas y los informes derivados de la evaluación de resiliencia resultan especialmente valiosos para llevar a cabo una autoevaluación y entender lo que se ha ejecutado de manera satisfactoria, así como las áreas que requieren mejoras y atención prioritaria en el contexto de la manufactura textil.

- **Establecimiento de responsabilidades**

La organización debe disponer de una estructura que gestione las funciones de toma de decisiones, funciones administrativas y funciones de gestión respuesta a incidentes. Este equipo debe estar conformado por personal interno, vinculado directamente por la organización.

En la *Tabla* 12, se plantea un escenario a manera de ejemplo del establecimiento de las responsabilidades en la organización.

Tabla 12. Establecimiento de responsabilidades en el SGCI

Rol	**Responsabilidades**
Director de Resiliencia	- Desarrollar y supervisar la estrategia de resiliencia y continuidad para el sector manufactura textil.
	- Asignar recursos y presupuesto para implementación y mantenimiento.
	- Colaborar con la alta dirección en decisiones estratégicas de continuidad.
	- Coordinar ejercicios de preparación y pruebas de recuperación.
Gerente de Continuidad	- Supervisar el plan de continuidad del negocio para operaciones textiles.
	- Identificar y priorizar procesos críticos de manufactura.
	- Coordinar la planificación y ejecución de recuperación ante desastres.
	- Establecer procedimientos de respuesta a incidentes específicos de la industria textil.
Coordinador de Comunicación de Crisis	- Gestionar la comunicación interna y externa durante incidentes en la manufactura textil.
	- Mantener relaciones con medios de comunicación y partes interesadas en la industria.
	- Informar a empleados y partes interesadas sobre la situación de la producción.
	- Coordinar la divulgación de información autorizada relacionada con textiles.
Responsable de TI para la Manufactura Textil	- Garantizar la integridad y disponibilidad de sistemas informáticos textiles.

	- Supervisar la recuperación de datos y aplicaciones esenciales para la producción.
	- Implementar medidas de seguridad cibernética específicas para la industria textil.
	- Colaborar en la planificación de respaldo y recuperación de datos textiles.
Coordinador de Recursos Humanos	- Asegurar la disponibilidad de personal clave en la producción textil durante crisis.
	- Facilitar la capacitación en procedimientos de emergencia para empleados textiles.
	- Gestionar las necesidades y bienestar de los trabajadores afectados en manufactura.
	- Colaborar en la planificación de rotación y reemplazo de personal textil.
Gerente de Operaciones Textiles	- Supervisar la continuidad de las operaciones de manufactura en el sector textil.
	- Coordinar la planificación de producción y el mantenimiento del inventario textil.
	- Identificar proveedores y recursos alternativos para mantener la producción.
	- Implementar prácticas de gestión de la cadena de suministro específicas para textiles.
Auditor de Seguridad para la Manufactura Textil	- Evaluar la seguridad de las instalaciones y sistemas de producción textil.
	- Identificar vulnerabilidades específicas y recomendar mejoras textiles.
	- Realizar auditorías periódicas de cumplimiento de políticas de seguridad en la manufactura textil.
	- Colaborar en la gestión de incidentes relacionados con la seguridad en textiles.
Equipo de Respuesta a Incidentes Textiles	- Actuar inmediatamente ante incidentes en el sector de manufactura textil.
(Equipo de seguridad TO)	- Coordinar actividades de respuesta y mitigación específicas para textiles.
	- Documentar incidentes textiles y aplicar lecciones aprendidas a mejoras futuras.

	- Implementar mejoras en políticas y procedimientos relacionados con textiles según sea necesario.

Nota. Ejemplo de matriz de responsabilidades del SGCI Fuente: Elaboración propia

- **Estrategia de resiliencia y continuidad: Análisis de impacto en el negocio (BIA)**

El análisis de impacto en el negocio (BIA, Business Impact Analysis) es una herramienta esencial para establecer una estrategia eficaz de continuidad y resiliencia en la industria textil. Su objetivo principal es identificar las necesidades críticas del negocio en términos de resistencia y recuperación.

Cuando se trata de servicios legalmente considerados esenciales, es fundamental analizar las consecuencias de cualquier interrupción, priorizando los riesgos de acuerdo con su importancia para la organización y asegurando su mitigación adecuada.

El propósito del BIA es primero identificar qué unidades de negocio, departamentos y procesos son vitales para la supervivencia de la empresa manufactura-textil. Luego, se estiman los impactos operativos y financieros de cada unidad, considerando escenarios adversos. Finalmente, se determina el tiempo máximo de recuperación asumible si ocurriese un desastre y los recursos necesarios para restaurar las operaciones en ese período.

Para la elaboración del BIA, es esencial definir parámetros clave, entre ellos:

- RTO (Recovery Time Objective): El tiempo necesario para recuperar actividades críticas bajo condiciones mínimas aceptables. Por ejemplo, si la plataforma de generación de energía debe recuperarse en un máximo de 2 horas, el RTO para ese proceso sería de 2 horas.
- MTD (Maximum Tolerable Downtime): El tiempo máximo que un proceso puede estar inactivo antes de causar efectos catastróficos en la empresa. Por ejemplo, si el proceso de monitorización en tiempo real no debe interrumpirse más de 6 horas, el MTD asociado es de 6 horas.
- RPO (Recovery Point Objective): El período máximo durante el cual se pueden perder datos antes de que tenga consecuencias inaceptables. Si la organización puede tolerar una pérdida de datos de hasta un día completo, el RPO sería de 24 horas.
- CTO (Containment Time Objective): El tiempo máximo tolerable para contener un fallo o ataque que podría provocar la pérdida de un servicio crítico.

La ejecución del BIA comienza con reuniones con las unidades de negocio involucradas, recopilando información esencial. El personal entrevistado proporciona detalles sobre procesos, requisitos de recuperación, dependencias con proveedores, clientes y otros aspectos relevantes. Todos estos elementos se documentan en el BIA.

El resultado del análisis es una lista priorizada de procesos o actividades con sus respectivos RTO, MTD, RPO y CTO. Esta información permite identificar las actividades críticas en el entorno industrial de la organización.

- **Procedimientos de resiliencia y continuidad**

La resiliencia y la continuidad de los sistemas de operación en el sector manufactura textil involucra una amplia gama de actividades diseñadas para mantener y recuperar los servicios críticos después de un evento adverso. Es importante destacar que la planificación de contingencias de los sistemas de operación debe ser parte integral de una estrategia más amplia que abarca la seguridad, la gestión de incidentes y la continuidad tanto de los procesos organizativos como de negocio, así como la recuperación ante desastres.

En última instancia, una organización debe emplear un conjunto de planes que asegure una respuesta, recuperación y continuidad adecuadas frente a perturbaciones que afecten a los sistemas de operación, los procesos de negocio, el personal y las instalaciones. Dado que existe una estrecha relación entre los sistemas de operación y los procesos de negocio que respaldan, se requiere una coordinación efectiva entre cada uno de estos planes durante su desarrollo y cambios, garantizando que las estrategias de recuperación estén alineadas y evitando duplicaciones de esfuerzos.

La planificación de la continuidad se enfoca principalmente en la capacidad de mantener las funciones y procesos críticos durante y después de un evento, centrándose en el negocio en sí. Por otro lado, los planes de contingencia se aplican típicamente a los sistemas de operación o información, detallando los pasos necesarios para recuperar, ya sea de manera manual o automatizada, la funcionalidad de sistemas específicos o partes de ellos en una ubicación determinada. La planificación de respuesta a incidentes, por su parte, se concentra en la detección, respuesta y recuperación frente a incidentes o eventos de seguridad tecnológica. Es por esto que la organización requiere de un proceso de respuesta a incidentes donde se gestionen las fases propuestas por el estándar NIST las cuales consisten en prepararse, detectar y analizar, contener y recuperar y finalmente el post-incidente.

DOMINIO 6: ESTABLECER LA GESTIÓN, REVISIÓN, MEJORA Y SOSTENIBILIDAD DEL SISTEMA DE GESTIÓN DE CIBERSEGURIDAD INDUSTRIAL.

Para garantizar el desarrollo y mantenimiento eficiente del SGCI en el sector de manufactura textil, es esencial contar con el sólido respaldo de la organización. Este respaldo se basa en la asignación adecuada de recursos humanos, documentación y una eficaz comunicación interna y externa, elementos que son fundamentales para establecer, implementar y mantener el SGCI de manera efectiva.

Estas capacidades deben ser proporcionadas de manera que respalden plenamente el desarrollo y la sostenibilidad del SGCI. A continuación, se identifican los requisitos clave:

- **Requisitos de competencia para el área de recursos humanos:**
  - Identificar las competencias necesarias para llevar a cabo cada actividad relacionada con la ciberseguridad industrial en el contexto de la manufactura textil.
  - Asegurar que el personal posea las competencias requeridas, basándose en su educación, formación y experiencia.
  - Tomar medidas, cuando sea necesario, para adquirir las competencias necesarias y evaluar su efectividad.
  - Mantener un registro documentado que demuestre la competencia del personal.
  - Fomentar la concientización en todo el personal acerca de la política de ciberseguridad, su contribución individual a la eficacia del SGCI y las implicaciones de las no conformidades con el SGCI.

- **Requisitos de Creación, Actualización y Control de Recursos Documentales:**
  - Incluir toda la documentación que la organización considere relevante para respaldar el SGCI en el sector manufactura textil.
  - Requisitos de Comunicación Interna y Externa del SGCI: Definir el contenido que debe ser comunicado y designar a los responsables de estas comunicaciones.
  - Planificar las comunicaciones relacionadas con el SGCI.
  - Establecer procesos efectivos de comunicación que permitan la fluidez y la efectividad en la difusión de información crítica.

La gestión de la documentación dentro del Sistema de Gestión de Ciberseguridad Industrial (SGCI) es crucial para garantizar el desarrollo y el mantenimiento del sistema, es por esto que la documentación debe estar controlada y debe garantizar los siguientes frentes:

- **Disponibilidad y Pertinencia de la documentación:**

Garantizar que la documentación esté disponible y sea apropiada para su uso en el momento y lugar necesarios en las operaciones textiles.

- **Protección de la documentación:**

Salvaguardar la documentación de manera adecuada contra amenazas como la pérdida de confidencialidad, el uso indebido o la alteración de su integridad, entre otras posibles vulnerabilidades.

Para administrar eficazmente esta información, la organización debe establecer:

- **Distribución, recuperación, acceso y uso apropiado de la documentación:**

Definir cómo se distribuirá la documentación, cómo se recuperará cuando sea necesario y quiénes tendrán acceso a ella de manera adecuada.

- **Almacenamiento y conservación de la documentación:**

Determinar los métodos de almacenamiento que aseguren la integridad y la disponibilidad de la documentación durante su ciclo de vida.

- **Control de cambios de la documentación:**

Establecer procedimientos para administrar las modificaciones y revisiones en la documentación, garantizando que siempre esté actualizada y relevante.

- **Retención y disposición de la documentación:**

Especificar el período durante el cual la documentación se mantendrá y cómo se eliminará o archivará apropiadamente al final de su utilidad.

En cuanto a los permisos de acceso a la información del SGCI, el responsable de la información, designado por la organización, debe definir:

  - Quiénes pueden consultar esta información.
  - Quién tiene la autoridad para acceder y realizar modificaciones en los documentos pertinentes.

Por otro lado, los requisitos de auditoría interna desempeñan un papel fundamental para asegurar que SGCI sea efectivo y cumpla con los estándares necesarios. Las auditorías internas son una herramienta esencial que la organización debe utilizar en intervalos planificados para recopilar información valiosa que garantice que los objetivos, controles, procesos y procedimientos relacionados con la ciberseguridad industrial estén en línea con los requisitos internos y externos. Para llevar a cabo las auditorías internas efectivas en el sector manufactura textil, es esencial tener en cuenta los siguientes aspectos:

- **Planificación del programa de auditoría:**

El programa de auditoría se debe planificar considerando la importancia de los procesos y áreas que serán auditados, y se debe basar en los resultados de auditorías previas.

- **Selección de auditores competentes:**

Los auditores designados deben asegurar que las auditorías se realicen de manera objetiva e imparcial, evitando auditar su propio trabajo.

- **Procedimientos documentados:**

La organización debe definir un procedimiento documentado que especifique las responsabilidades, requisitos y dirección de las auditorías, incluyendo la emisión de un informe con los resultados obtenidos.

- **Criterios y alcance de la auditoría:**

Se deben establecer claramente los criterios y el alcance de la auditoría para enfocarse en los aspectos más relevantes de la ciberseguridad industrial en la manufactura textil.

- **Ejecución imparcial:**

Las auditorías deben llevarse a cabo de manera objetiva e imparcial, garantizando una evaluación justa y precisa.

- **Comunicación de resultados:**

Los resultados de la auditoría deben comunicarse de manera efectiva a la alta dirección, asegurando que estén al tanto de cualquier hallazgo significativo.

- **Gestión de evidencias documentadas:**

Se debe mantener una documentación adecuada de las pruebas y evidencias relacionadas con la implementación de los programas de auditoría.

- **Responsabilidades:**

Las responsabilidades en torno a las auditorías internas deben estar definidas claramente, incluyendo la planificación, los requisitos, la presentación de resultados y la gestión de registros.

La alta dirección de la organización es responsable de garantizar que las áreas auditadas tomen las acciones necesarias para abordar cualquier no conformidad identificada durante la auditoría interna y que se presenten explicaciones claras sobre las causas de dichas no conformidades. Además, se debe llevar a cabo un seguimiento de las acciones realizadas, incluyendo una verificación de los resultados obtenidos.

DOMINIO 7: PROMOCIÓN DE LA CULTURA DE CIBERSEGURIDAD INDUSTRIAL.

Este dominio se enfoca en fomentar una conciencia y cultura a nivel de ciberseguridad. Busca educar, sensibilizar y promover practicas seguras relacionadas con la tecnología y la información. En la *Figura* 10 se propone la estructura de promoción de la cultura que la organización debe seguir, adicionalmente se definen cada uno de sus componentes.

Figura 10. Promoción de la cultura de ciberseguridad industrial

Nota. Pilares de la promoción de la cultura de ciberseguridad Fuente: Elaboración propia

- **Planeación**

La organización debe identificar los objetivos de la promoción de la cultura de ciberseguridad industrial, como la concientización de los empleados, la implementación de buenas prácticas y la protección de la información y activos de la empresa. En esta fase es importante determinar el público objetivo de la promoción, como empleados de la empresa, proveedores, clientes y socios comerciales. Posterior a estas actividades, se debe establecer el calendario de actividades y los recursos necesarios para llevar a cabo la promoción de la cultura de ciberseguridad industrial.

A continuación, se comparten algunos ejemplos para la identificación de los objetivos:

- Mejorar la concientización general en ciberseguridad: se busca crear una mayor concientización entre los empleados sobre la importancia de proteger los recursos y sistemas de la organización contra posibles amenazas cibernéticas. Esto implica comprender los riesgos y saber cómo actuar para prevenir incidentes.
- Desarrollar habilidades y conocimientos: la formación tiene como propósito capacitar a los trabajadores en habilidades y conocimientos que les permitan desempeñar sus tareas de manera eficiente y segura desde una perspectiva de ciberseguridad.
- Formación en ciberseguridad para el personal de control y automatización industrial: aquellos empleados relacionados con sistemas de control y automatización industrial deben recibir formación específica en ciberseguridad y tecnologías de la información para garantizar la protección de los sistemas críticos.
- Formación para el personal de tecnologías de información: los profesionales de tecnologías de información que trabajan en el entorno industrial, incluyendo la automatización y control industrial, también requieren formación en aspectos específicos de este entorno. Esto incluye la comprensión de la seguridad física, procesos industriales y tecnologías de automatización.

- **Diseño de contenidos**

La organización debe **c**rear materiales educativos y de concientización, como presentaciones, infografías, videos y folletos, que expliquen los conceptos básicos de la ciberseguridad industrial, los riesgos asociados y las medidas de protección que deben ser tomadas. Adicionalmente, debe adaptar los contenidos a la audiencia específica, utilizando un lenguaje claro y sencillo que sea fácil de entender para todos los niveles de conocimiento. Cómo recomendación, se pueden incluir ejemplos y casos reales de incidentes de ciberseguridad industrial para resaltar la importancia de la protección de los sistemas y la información.

Complementando el desarrollo de contenidos, se propone algunos ejemplos a seguir:

- Comunicación en intranet y plataformas en línea: utilizando boletines, correos electrónicos y otros recursos en línea para transmitir información relevante.
- Material impreso: mediante la colocación de carteles informativos en áreas clave de la organización.
- Avisos de audio: empleando mensajes de audio para recordar la importancia de la ciberseguridad.
- Videos educativos: utilizando videos que muestren casos de incidentes de ciberseguridad, particularmente aquellos de relevancia pública.

- **Implementación**

En esta fase es importante realizar talleres y sesiones de capacitación para el grupo objetivo, empleados, proveedores, clientes y socios comerciales, utilizando los materiales educativos creados. Se debe fomentar la participación de los empleados en la promoción de la cultura de ciberseguridad industrial, animándolos a compartir buenas prácticas y a reportar cualquier incidente o actividad sospechosa.

Es importante compartir los procedimientos y políticas internas que promuevan la protección de la información y los sistemas, como el uso de contraseñas seguras, la actualización regular de los sistemas y la realización de copias de seguridad.

- **Medición**

Evaluar el impacto de la promoción de la cultura de ciberseguridad industrial es importante, se deben establecer los mecanismos como por ejemplo la realización de encuestas o cuestionarios antes y después de las actividades de capacitación. Los resultados de la medición deben ser analizados dependiendo de las métricas definidas, se propone hacer ejercicios de phishing o de ataques controlados para verificar el aumento en la conciencia de la ciberseguridad industrial.

Las acciones de formación y concientización deben ser continuas en el tiempo para garantizar la retención de conocimientos y fomentar las prácticas de seguridad industrial en los empleados. El responsable del sistema de gestión de ciberseguridad industrial debe planificar y programar estas acciones en conjunto con el área de recursos humanos como parte integral de la estrategia de seguridad.

FASE III - VALIDACIÓN DEL SISTEMA DE GESTIÓN DE CIBERSEGURIDAD INDUSTRIAL.

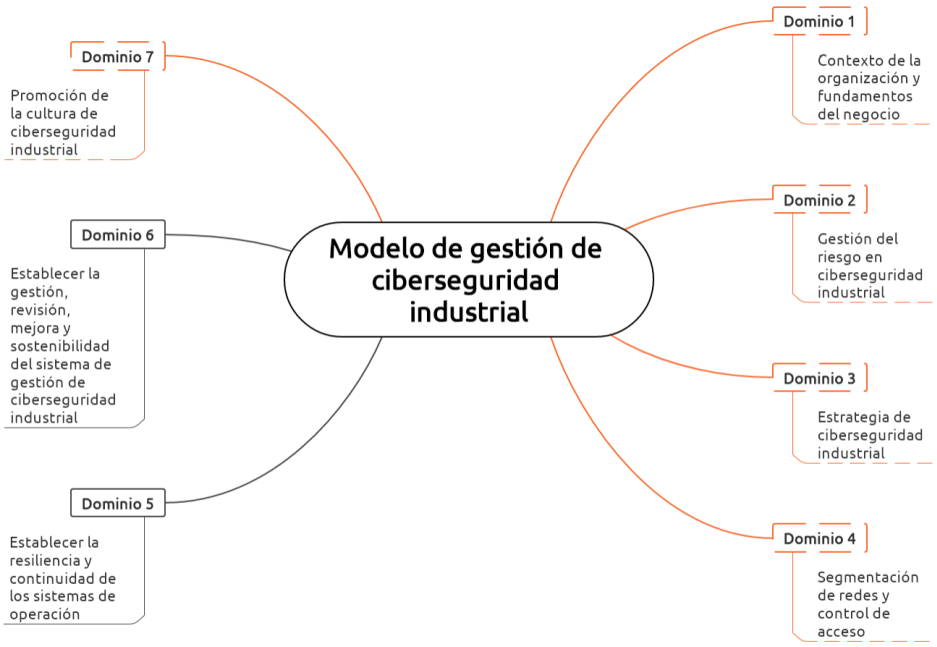
La validación del sistema de gestión de ciberseguridad industrial en el sector manufactura-textil es un proceso que requiere la implicación y colaboración de todos los miembros de la organización. En esta fase, se da cumplimiento al tercer objetivo “Validar el sistema de gestión de ciberseguridad industrial enfocado en las TO a través de un caso de estudio en una empresa del sector manufactura-textil”. En este contexto, se ha colaborado estrechamente con una empresa del sector manufactura-textil que ha accedido a participar en la implementación y validación del SGCI propuesto en el presente proyecto de grado.
Para respetar los acuerdos de confidencialidad y privacidad, la organización ha optado por no revelar su nombre. La colaboración con esta empresa ha sido fundamental, ha permitido llevar a cabo un caso de

estudio real y práctico que demuestra la aplicabilidad y eficacia del SGCI en un entorno industrial específico.

Se realizó una reunión de apertura con las diferentes áreas de la organización involucradas en el proyecto, en esta sesión se socializó el presente proyecto de grado y se presentó el SGCI diseñado en la fase II. En conjunto con la organización, se limitó el alcance de la validación del sistema de gestión de acuerdo a lo siguiente:

- Se determinó abordar cinco dominios los cuales se identifican en la *Figura* 11 (Dominio 1: Contexto de la organización y fundamentos del negocio, Dominio 2: Gestión del riesgo en ciberseguridad industrial, Dominio 3: Estrategia de ciberseguridad industrial, Dominio 4: Segmentación de redes y control de acceso, Dominio 7: Promoción de la cultura de ciberseguridad industrial)
- El dominio 2, correspondiente a la gestión del riesgo, se realizará específicamente para el proceso industrial de bondeado.
- Para el dominio 2, se determinó la realización de dos escenarios de gestión de riesgos, uno antes y otro posterior a la validación del SGCI. Esto permitirá identificar si la validación del sistema de gestión efectivamente ayudó a mitigar los riesgos de ciberseguridad industrial en la organización.

Figura 11. Dominios que se abordarán en la validación del SGCI



Nota. Dominios del sistema de gestión de ciberseguridad industrial que se abordarán en conjunto con la organización
Fuente: Elaboración propia

DOMINIO 1: CONTEXTO DE LA ORGANIZACIÓN Y FUNDAMENTOS DEL NEGOCIO

El objetivo de este documento fue proporcionar una descripción exhaustiva de los aspectos clave del contexto de la organización. Esta descripción permitió la identificación de los fundamentos del negocio que justifican la necesidad de implementar el Sistema de Gestión de Ciberseguridad Industrial (SGCI).

Adicionalmente, se establecieron los esfuerzos necesarios para la implementación del sistema. En este documento se estableció la misión de la organización, se plasmaron los objetivos estratégicos de la organización, se identificaron los beneficios de la implementación del SGCI y finalmente, la organización definió los recursos a nivel de personas y presupuesto para la implementación del SGCI.

Este dominio tuvo lugar a diferentes sesiones de trabajo, como resultado final, se diligenció el documento "Anexo 08 - Dominio 1 - Contexto de la organización". El documento fue comunicado a todos los empleados de la organización por correo electrónico y quedó publicado en la intranet para que sea consultado por el personal que lo requiera.

Con la implementación del dominio 1, se identifica que la organización está adoptando un enfoque integral hacia la ciberseguridad industrial, incorporando la ciberseguridad en su planificación estratégica, asignando recursos y comunicando eficazmente su enfoque a todo el personal. Esto es esencial para proteger sus operaciones en el sector manufactura-textil y garantizar la continuidad de sus operaciones en un entorno industrial cada vez más digital y conectado.

DOMINIO 2: GESTIÓN DEL RIESGO EN CIBERSEGURIDAD INDUSTRIAL

Este dominio se identificó como el más complejo desarrollado en conjunto con la organización, esto debido a que no se tenían mapeados los diferentes insumos para la gestión del riesgo. Sin embargo, se realizaron diferentes sesiones de trabajo y en conjunto se diligenciaron y se crearon cada uno de los anexos propuestos en la construcción del SGCI. A continuación se comparten los anexos desarrollados:

Identificación de activos:

Anexo 09 - Dominio 2 - Inventario de activos industriales

Identificación de amenazas:

Anexo 10 - Dominio 2 - Inventario de amenazas

Identificación de vulnerabilidades:

Anexo 11 - Dominio 2 - Inventario de vulnerabilidades

Identificación de controles existentes:

Anexo 12 - Dominio 2 - Inventario de controles existentes

Análisis, gestión y seguimiento al riesgo:

Anexo 13 - Dominio 2 - Gestión de riesgo

Para el primer escenario de riesgo, se construyó el documento "Anexo 13 - Dominio 2 - Gestión de riesgo", durante su desarrollo y como se indicó en el alcance, se determinó realizar el análisis de riesgos al proceso de bondeado, para ello se determinaron los activos críticos y su clasificación, esto con el fin de identificar el nivel de criticidad de los activos a evaluar. Se tuvo en cuenta que a nivel de las TO, la prioridad gira entorno a la disponibilidad de los activos como se evidenció en el desarrollo de la fase I del presente proyecto.

Posterior a la identificación y evaluación de los activos, se realizó la verificación de los controles actuales en el ambiente TO, en este aspecto se evidenció la carencia de controles para este ambiente pues todos sus controles estaban orientados al ambiente TI.

La organización no tenía identificadas las amenazas y vulnerabilidades, por lo tanto, se llevó a cabo la identificación de estos aspectos teniendo en cuenta los escenarios que podrían afectar los activos del proceso industrial.

Una vez se tuvieron todos los insumos para la gestión del riesgo, se determinó el escenario de riesgo en la *Tabla* 13, allí se evidencia las amenazas más representativas que pueden explotar a los activos críticos del proceso de bondeado.

Tabla 13. Escenario de riesgo entre las amenazas y los activos.

AMENAZAS \ ACTIVOS	Bondeadora	Cortadora extremos	Cortadora vertical	Fusionadora	Bascula	Dinamómetro de fuerza	PLC centralizador	Switch	Access Point	Base de datos	Aplicación	Revisora de tela	Información	Personas
Fallo de comunicación a nivel de red		x	x	x	x	x	x	x	x	x	x	x		
Modificación de información en tránsito						x	x			x	x			
Suplantación de identidad							x			x	x			x
Acceso no autorizado							x			x	x			
Malware							x			x	x			
Phishing industrial														x
Ataques de denegación de servicio (DDoS)	x	x	x	x	x	x	x	x	x	x	x	x	x	
Software obsoleto	x	x	x				x					x		
Ingeniería social														x
Abuso de privilegios							x	x	x					x
Fuga de información														x

Nota. Escenario de riesgo elaborado entre las amenazas y los activos Fuente: Elaboración propia

Posterior al escenario entre las amenazas y los activos, en el Anexo 13 – Dominio 2 – Gestión de riesgos en la hoja calificación-control se realiza la calificación de los controles que actualmente tiene la organización implementados. Tal como se indicó previamente, la organización no cuenta con controles para el ambiente TO, haciendo de este ambiente un entorno altamente riesgoso para la compañía. En la *Tabla* 14, se comparte el resultado final del primer análisis de riesgos donde se identifica que la organización cuenta con 42 riesgos inadmisibles y 8 riesgos inaceptables, esto indica que, del total de los 50 riesgos identificados, el 84% son inadmisibles y el 16% son inaceptables.

Tabla 14. Escenario de riesgo en la organización

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					(19) - (26) - (41) - (42) - (43) - (45) - (49) - (50) -
Probable	4		(4) - (5) - (11) - (12) - (31) - (32) - (38) -	(44) -	(1) - (2) - (3) - (8) -	(6) - (7) - (9) - (10) - (13) - (14) - (15) - (16) - (17) - (18) - (20) - (21) - (22) - (23) - (24) - (25) - (27) - (28) - (29) - (30) - (33) - (34) - (35) - (36) - (37) - (39) - (40) - (46) - (47) - (48) -
Posible	3					
Improbable	2					
Raro	1					

Nota. Escenario de riesgo en la organización posterior a la gestión de riesgos Fuente: Elaboración propia

En la *Tabla* 15, se identifica la distribución porcentual del escenario de riesgo en la organización del sector manufactura-textil, como se puede visualizar, los riesgos en el proceso de bondeado se centran en la zona inaceptable e inadmisible.

Tabla 15. Distribución porcentual del escenario de riesgo en la organización

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	0,00	0
Tolerable	0,00	0
Inaceptable	7,14	2
Inadmisible	92,86	26

Nota. Distribución porcentual del escenario de riesgo en la organización Fuente: Elaboración propia

Posterior a la generación de la matriz de riesgos, se trabajó en conjunto con la organización para diseñar el plan de tratamiento, en este ejercicio se definió el tratamiento de los riesgos inaceptables e inadmisibles, se generó la descripción del plan, se diseñó el plan de monitoreo del plan de tratamiento, se identificaron los responsables y finalmente se indicó el resultado esperado. Esta información se puede visualizar en el Anexo 13 – Dominio 2 – Gestión de riesgo en la hoja titulada “Tratamiento”.

La ejecución de la evaluación de riesgos se presentó a la alta dirección de la organización. Tras la revisión, se determinó la necesidad de avanzar con la implementación del Sistema de Gestión de Ciberseguridad Industrial propuesto. Además, se acordó llevar a cabo una intervención inmediata con un enfoque en la gestión de riesgos. Esta decisión se fundamentó en que la mayoría de los riesgos se encuentran en la zona inadmisible y en caso de materializarse, podrían afectar de manera significativa a la organización.

DOMINIO 3: ESTRATEGIA DE CIBERSEGURIDAD INDUSTRIAL

La estrategia de ciberseguridad se apoya completamente en el contexto y los fundamentos del negocio donde claramente se identifica la estrategia de la compañía y sus necesidades, partiendo de estos elementos, se crearon los siguientes 3 pilares fundamentales:

- Ámbito del Sistema de Gestión de Ciberseguridad Industrial (SGCI)
- Política de Ciberseguridad Industrial
- Estructura de Ciberseguridad

El desarrollo del presente dominio se realizó en el "Anexo 14 - Dominio 3 - Estrategia de ciberseguridad industrial". Esta estrategia fue compartida a todos los empleados de la compañía y fue alojada en la intranet de la organización para que esté disponible para el personal en el momento en que lo requiera.

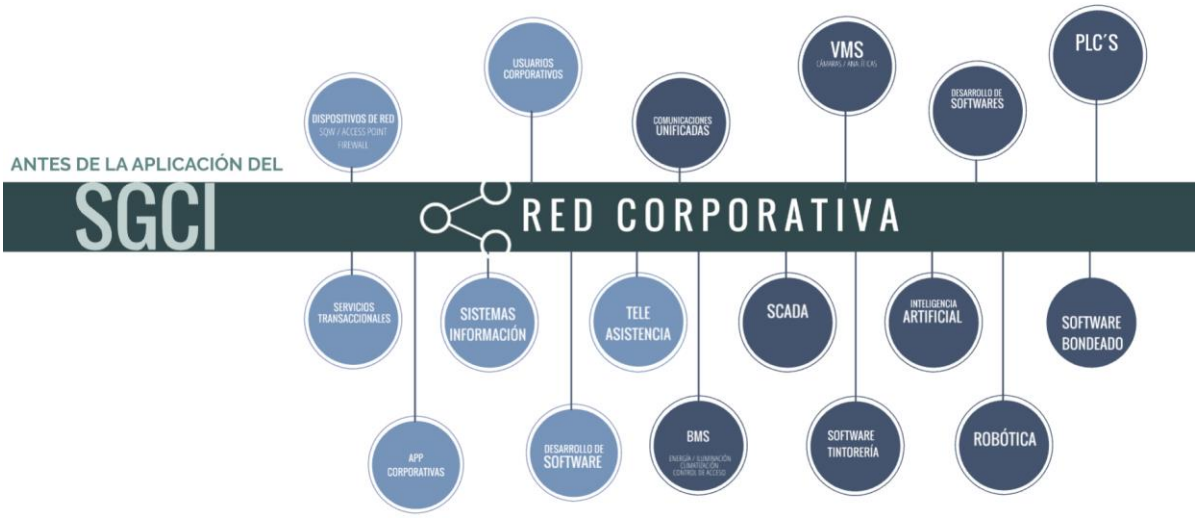
Durante la ejecución del dominio 3 se logró modificar el organigrama de la organización debido a que antes de la aplicación del SGCI la coordinación de seguridad se encontraba dentro de la jefatura de plataforma informática. Gracias a la validación del SGCI se logró separar la coordinación al mismo nivel de las jefaturas. Este cambio permitirá empoderar aún más al proceso de ciberseguridad y se empieza a identificar una mejor estructura con énfasis en la gestión de incidentes y políticas a nivel industrial.

DOMINIO 4 SEGMENTACIÓN DE REDES Y CONTROL DE ACCESO

La segmentación de redes y el control de acceso son pilares importantes en la gestión de la ciberseguridad. Estos conceptos se han vuelto esenciales a medida que la infraestructura de red se ha vuelto más compleja y los riesgos cibernéticos continúan evolucionando. En el presente dominio, se realizaron diferentes sesiones de trabajo en conjunto con las áreas de TI y TO de la organización con el fin de identificar la arquitectura actual a alto nivel, este insumo permitió poder ajustar la arquitectura a las definiciones iniciales y buenas prácticas propuestas por la norma ISA95 / IEC 62442 bajo el modelo de Pardue.

En la *Figura* 12, se identifica la arquitectura antes de la implementación del SGCI en la organización.

Figura 12. Arquitectura antes de la implementación del SGCI

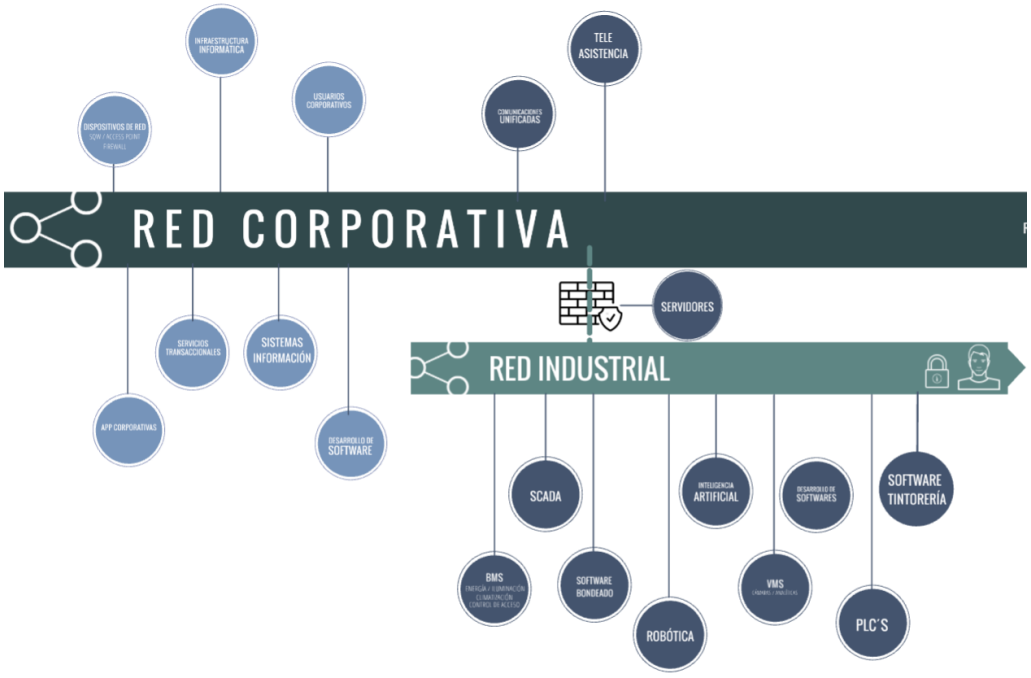


Nota. Arquitectura a alto nivel antes de la implementación del SGCI Fuente: Elaboración propia

Cómo se evidencia en la *Figura* 12, la organización cuenta con una red corporativa donde se conectan los diferentes servicios y activos tecnológicos. Esta arquitectura presenta diferentes riesgos de ciberseguridad debido a que se están utilizando los mismos equipos para la conexión de la infraestructura crítica, por esta identificación, la arquitectura no cumple con las recomendaciones y definiciones de la IEC 62443 enfocada en las infraestructuras críticas. Al tener en una misma red los elementos de TI y TO, la organización se expone a altos riesgos debido a que cómo lo hemos visto en el presente proyecto, los activos TO son elementos muy vulnerables y pueden llegar a comprometer la red corporativa. Adicionalmente, se identifica que la red industrial no cuenta con controles internos para la segmentación de redes, no cuenta con firewall ni switch de manera independiente que permitan realizar los respectivos controles de acceso a los dispositivos.

En la *Figura* 13, se presenta la arquitectura diseñada y expuesta a la organización posterior a la implementación del SGCI específicamente en el dominio 4, bajo los criterios propuestos en el documento. Esta arquitectura se propuso a alto nivel como medida inicial para la segmentación de redes e implementación de control de acceso.

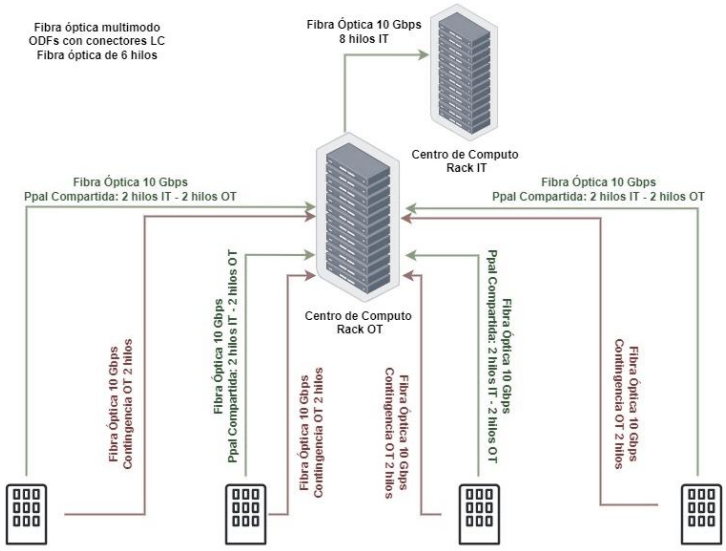
Figura 13. Arquitectura después de la implementación del SGCI



Nota. Arquitectura a alto nivel después de la implementación del SGCI Fuente: Elaboración propia

Para lograr la segmentación de la red industrial, fue necesario realizar la conexión independiente de cada uno de los centros de cableado donde se conectan los activos TO, para esta segmentación se propuso el diseño en conexiones de fibra óptica identificados en la *Figura* 14. Este diseño fue aprobado e implementado por la organización.

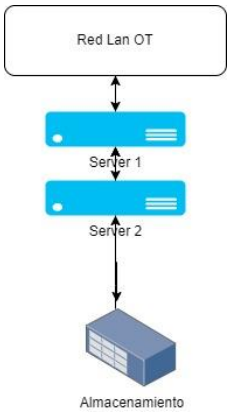
Figura 14. Diseño de conexión de centros de cableado



Nota. Arquitectura de la conexión de los centros de cableado de la red TO Fuente: Elaboración propia

Para el dimensionamiento de los equipos y el licenciamiento necesario para esta implementación, a nivel de servidores, se tuvieron en cuenta las capacidades de procesamiento, de almacenamiento, de tarjetas de red y de comunicación, adicionalmente se planteó alta disponibilidad para este esquema tal como se puede visualizar en la *Figura* 15.

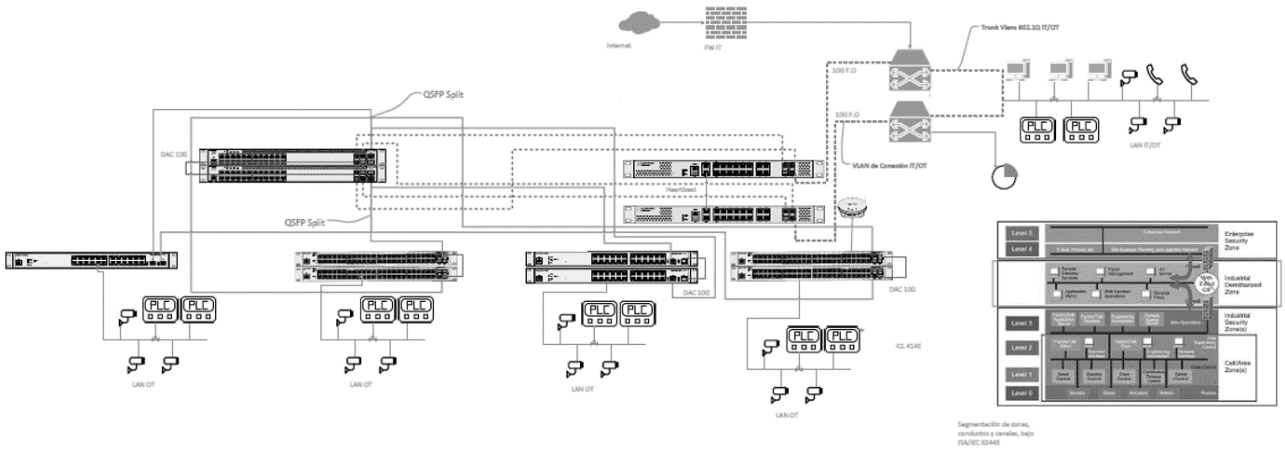
Figura 15. Arquitectura de servidores OT



Nota. Arquitectura de servidores OT Fuente: Elaboración propia

A nivel de switchs, se realizó un escaneo en los switchs de TI con el fin de determinar las cantidades de los activos críticos que estaban conectados en la red corporativa, con la identificación de estas cantidades se realizó el dimensionamiento y se incluyeron los firewalls en alta disponibilidad para segmentar las redes entre el entorno TO y TI como se puede visualizar en la *Figura* 16, esta arquitectura TO fue propuesta, aprobada e implementada en conjunto con la organización siguiendo los lineamientos del presente SGCI enmarcado en la norma IEC 62443 bajo el estándar ISA95 para el dominio 4 correspondiente a la segmentación de redes y control de acceso

Figura 16. Arquitectura después de la implementación del SGCI



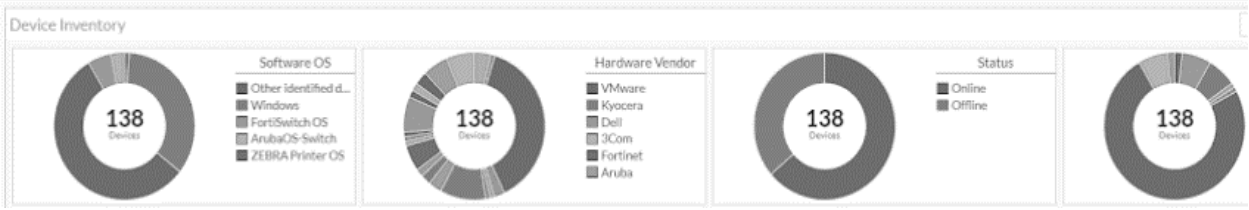
Nota. Arquitectura a bajo nivel después de la implementación del SGCI Fuente: Elaboración propia

La arquitectura plasmada en la *Figura* 16 contempla la segmentación de redes con dos firewalls en alta disponibilidad, enlaces redundantes para garantizar doble anillo de conectividad y alta disponibilidad entre sus elementos. Se implementaron dos switchs core centralizadores de todos los centros de cableado y se conectaron a 9 switchs de acceso donde finalmente se conectaron los activos TO.

En el proceso de implementación se instalaron firewalls de última generación en alta disponibilidad, estos elementos permitieron segmentar las redes TI y TO. El licenciamiento adquirido y propuesto permitió habilitar características de TO el cual habilitó la visibilidad sobre los activos y los protocolos industriales. Para dar cumplimiento al control de acceso propuesto desde el diseño del SGCI, se realizó la segmentación de los centros de cableado para que el ambiente TO quedara totalmente aislado del ambiente TI. Se implementaron switchs con funcionalidades de control de acceso los cuales permitieron lograr la identificación, autenticación, autorización y tener la trazabilidad de las conexiones a los activos TO.

En la *Figura* 17 se identifica, posterior a la implementación, el inventario de activos industriales durante el proceso de conexión a la red TO, esta funcionalidad permitió identificar en tiempo real los activos del ambiente TO lo cual no era visible para la organización antes de la validación del SGCI.

Figura 17. Inventario de activos industriales

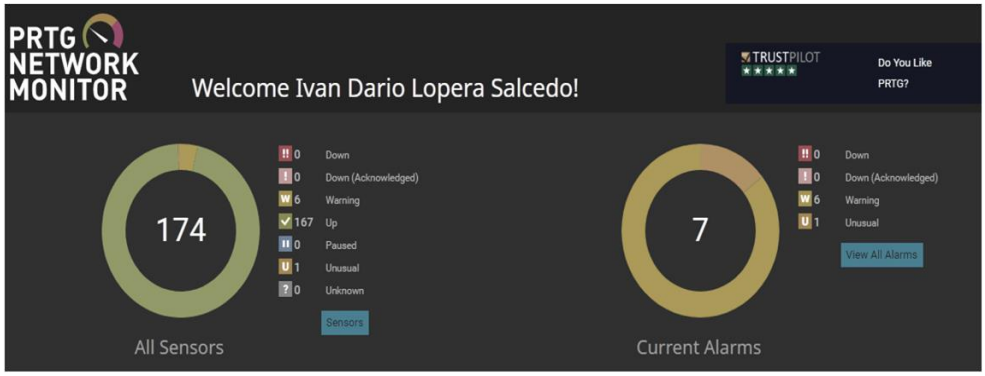


Nota. Inventario de activos industriales en tiempo real desde la plataforma centralizada Fuente: Elaboración propia

Luego de habilitar las funcionalidades de visibilidad, se realizaron las configuraciones de las reglas de entrada y salida del ambiente TO en los firewalls, esta actividad fue ejecutada para cada uno de los dispositivos industriales de la infraestructura crítica. También se ajustaron las políticas de control de acceso en los firewalls y en los switchs con el fin de garantizar el acceso a quien en realidad lo requiere. A nivel de firewall, se habilitaron las siguientes funcionalidades las cuales permiten fortalecer las capacidades de seguridad de la red: antivirus con firmas de TO, filtrado web, control de aplicaciones, prevención de intrusos, filtrado de correo, prevención de pérdida de información y aplicaciones web. Se identificó que en la funcionalidad de prevención de pérdida de información se debe realizar una tarea exhaustiva correspondiente al etiquetado de la información confidencial, privada y pública, sin esta identificación la característica no funciona de manera adecuada. Esta actividad queda pendiente por desarrollar por parte de la organización para que el módulo opere correctamente.

La arquitectura propuesta en la *Figura* 16 se complementa con la incorporación de un software de monitoreo de red, este software identificado en la *Figura* 18, permite identificar en tiempo real el estado de los activos críticos del ambiente TO (previamente vinculados a la herramienta). En conjunto con la organización y tomando como referencia la política de ciberseguridad industrial, se define que el monitoreo se realizará sobre los activos críticos de TO como servidores, firewalls, switch, PLC, entre otros.

Figura 18. Monitoreo de activos industriales



Nota. Monitoreo de activos industriales en tiempo real desde la plataforma PRTG centralizada Fuente: Software PRTG Network Monitor.

Con la anterior implementación se culmina el dominio 3, se da cumplimiento a las buenas prácticas propuestas en el SGCI donde se aborda la segmentación de redes y la implementación del control de acceso.

DOMINIO 7: PROMOCIÓN DE LA CULTURA DE CIBERSEGURIDAD INDUSTRIAL

Durante el desarrollo de la implementación del modelo de gestión de ciberseguridad industrial se trabajó de manera directa en el presente dominio, cada una de las actividades realizadas en la organización ha requerido pasar por cada uno de los pilares planteados en la promoción de cultura de ciberseguridad industrial propuestos en la *Figura* 19 y se ha tenido que compartir con las diferentes áreas que intervienen en el proyecto y los empleados de la organización.

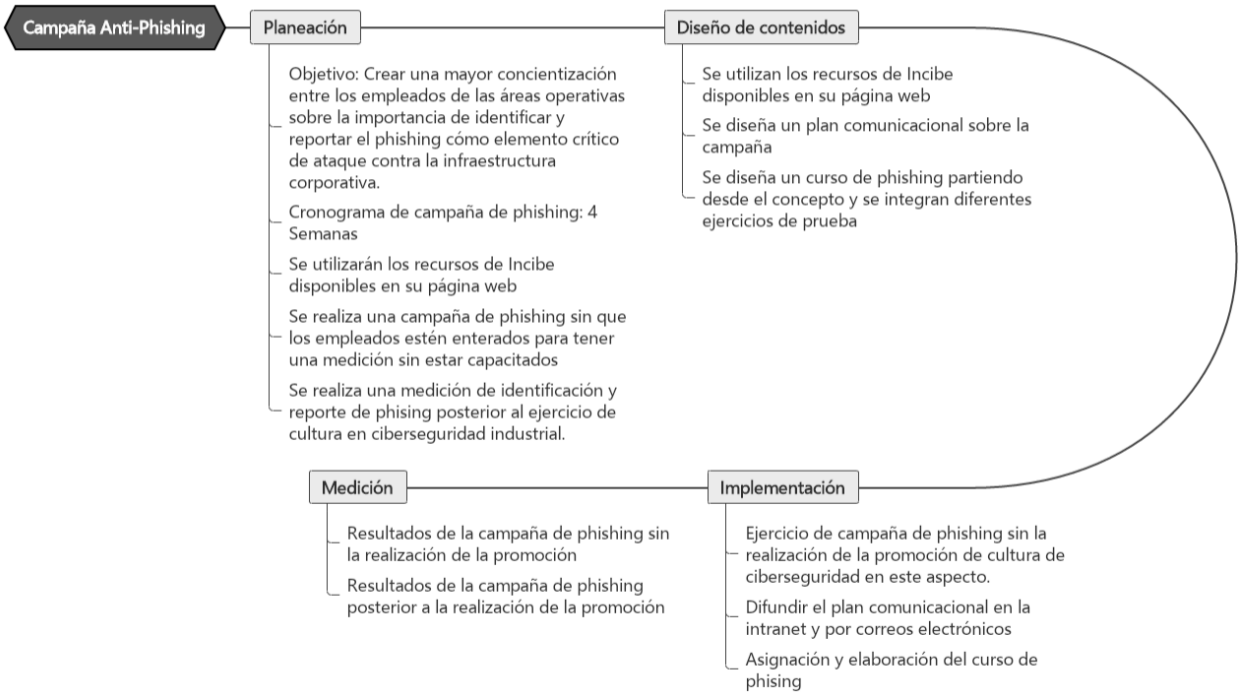
Figura 19. Promoción de la cultura de ciberseguridad industrial

Nota. Dominio 7 promoción de la cultura de ciberseguridad industrial Fuente: elaboración propia

Cómo valor agregado al dominio 7, se definió en conjunto con la organización reforzar la concientización de los usuarios ante un escenario de phishing industrial, esto debido a que se identificó que en la organización no se han realizado campañas respecto al escenario anti-phishing para el ambiente TO, el cual es crítico en la actualidad del entorno industrial.

En la *Figura* 20, se comparte el desarrollo de la campaña anti-phishing diseñada y ejecutada en conjunto con la organización y se definió hacer dos campañas, una antes de la aplicación del SGCI y otra posterior, esto con el fin de determinar la eficacia del modelo.

Figura 20. Campaña de Anti-Phishing



Nota. Campaña de anti-phishing realizada en la organización Fuente: elaboración propia

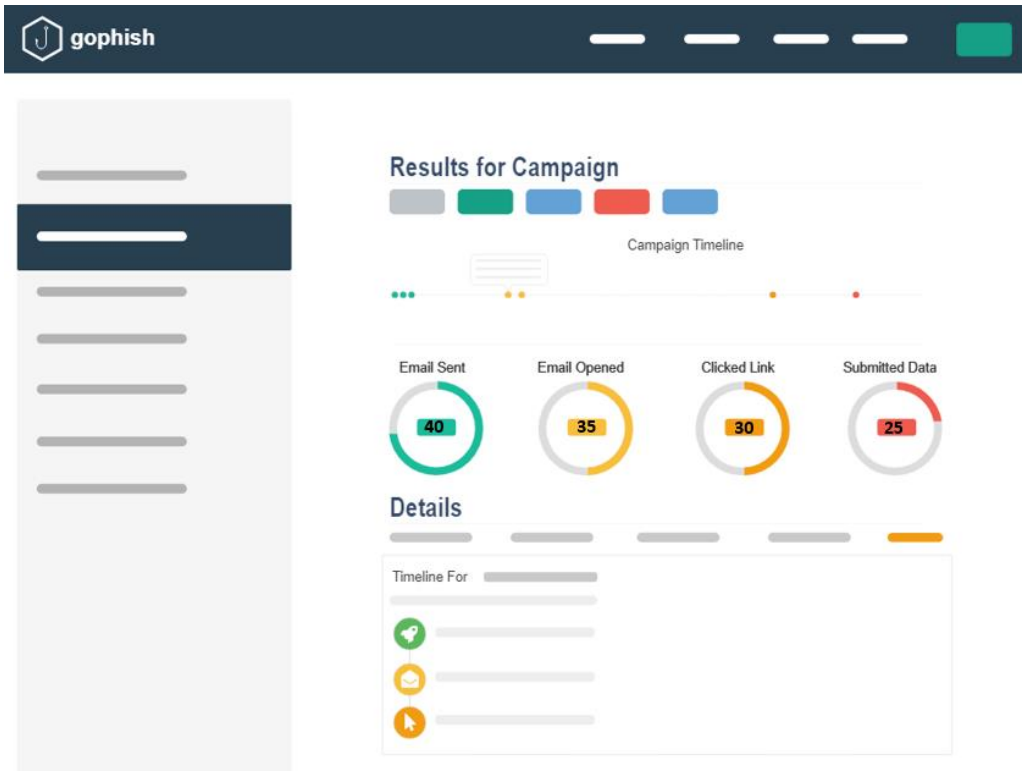
Para la campaña anti-phishing se utilizó la plataforma GoPhish, esta es una herramienta de phishing de código abierto utilizada para llevar a cabo campañas de phishing y pruebas de concientización en seguridad en entornos controlados. Fue diseñada para ser utilizada por profesionales de seguridad cibernética, ingenieros de seguridad y equipos de pruebas de penetración para evaluar la susceptibilidad de una organización a ataques de phishing y mejorar la concientización de los empleados en materia de seguridad. Esta plataforma permite realizar:

- Creación de Campañas de Phishing permitiendo a los usuarios crear campañas de phishing simuladas que pueden incluir correos electrónicos de phishing, páginas web falsas y otros elementos diseñados para engañar a los destinatarios.
- Plantillas Personalizadas permitiendo ofrecer la capacidad de personalizar plantillas de correo electrónico y páginas web para que coincidan con los objetivos de la campaña.
- Seguimiento de correos electrónicos proporcionando la capacidad de realizar un seguimiento de los correos electrónicos enviados, incluyendo la detección de apertura de correos electrónicos y clics en enlaces.
- Informes y estadísticas con informes detallados que muestran el rendimiento de la campaña, incluyendo el número de destinatarios comprometidos y las acciones realizadas por los destinatarios.
- Pruebas de concientización en seguridad identificando vulnerabilidades y educando a los empleados sobre los riesgos del phishing.
- Personalización avanzada permitiendo a los usuarios personalizar la URL de destino, las páginas de inicio de sesión y otros elementos de la campaña.

- Integración con otras herramientas y servicios de seguridad para mejorar la eficacia de las pruebas de phishing y la respuesta a incidentes.

En la *Figura* 21, se comparten los resultados de la campaña de anti-phishing antes de la aplicación del SGCI bajo el dominio 7 correspondiente a la promoción de cultura de ciberseguridad industrial.

Figura 21. Resultados del ejercicio de phishing antes de la promoción



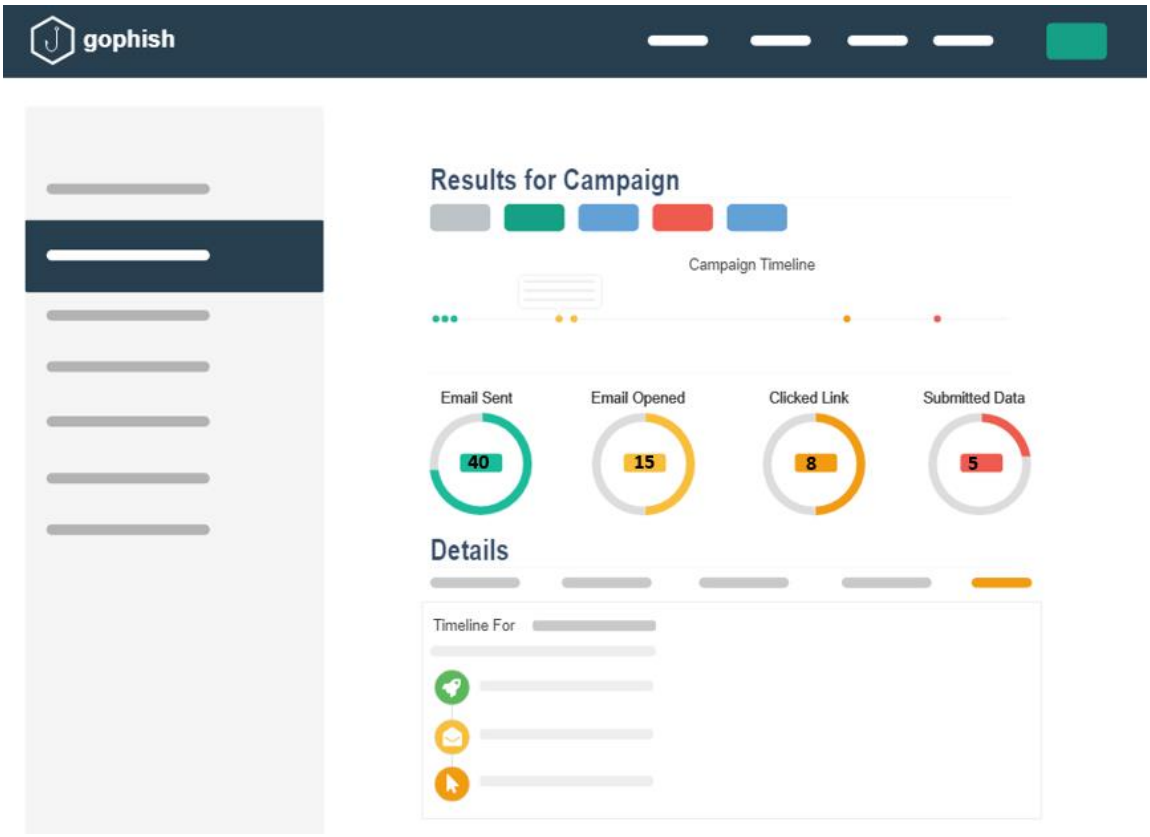
Nota. Campaña de phishing realizada en la organización Fuente: elaboración propia

Como se evidencia en los resultados de la *Figura* 21, se enviaron 40 correos hacía los buzones de los empleados de las áreas de la operación industrial de los cuales:

- El 88% de los empleados abrieron el correo (35 empleados)
- El 75% de los empleados ingresaron al link malicioso (30 empleados)
- El 63% de los empleados expusieron sus credenciales de acceso (25 empleados)

Posterior a la implementación del SGCI donde se realizó el plan de promoción de cultura de ciberseguridad industrial propuesto en el dominio 7, se volvió a realizar el mismo ejercicio con personal diferente del área de operaciones. Los resultados se pueden visualizar en la *Figura* 22.

Figura 22. Resultados del ejercicio de anti-phishing después de la aplicación del SGCI



Nota. Campaña de anti-phishing realizada en la organización posterior a la implementación del SGCI Fuente: elaboración propia

Como se evidencia en los resultados de la *Figura* 22, se enviaron 40 correos hacía los buzones de los empleados de las áreas de la operación industrial de los cuales:

- El 38% de los empleados abrieron el correo (15 empleados)
- El 20% de los empleados ingresaron al link malicioso (8 empleados)
- El 13% de los empleados expusieron sus credenciales de acceso (5 empleados)

Los ejercicios realizados en la *Figura* 21 y 22, permitieron identificar que gracias a la implementación del SGCI enfocado en el dominio 7 “Promoción de la cultura de ciberseguridad industrial”, se contribuye a fortalecer la concientización de los empleados y a minimizar el riesgo enfocado en los errores de las personas. Del 63% de exposición de credenciales de acceso compartidas por los empleados en el primer escenario, se logró reducir al 13% de exposición en el segundo escenario, estos valores permiten determinar que efectivamente el SGCI permite fortalecer la postura de ciberseguridad a través de ejercicios de concientización a los empleados de la organización.

Una vez ejecutados los dominios pactados en la *Figura* 11 con la organización, se procedió a realizar nuevamente el escenario de riesgos con el fin de verificar si el SGCI enfocado a las tecnologías de la

operación permitió mitigar los riesgos en las plataformas industriales del sector manufactura-textil, esta validación se documentó en el "Anexo 15 - Dominio 2 - Gestión de riesgo con SGCI".

En la *Tabla* 16, se comparte el resultado final del segundo análisis de riesgos. Se puede identificar que la organización cuenta con 4 riesgos inadmisibles, 33 riesgos inaceptables, 7 riesgos tolerables y 6 riesgos aceptables, esto indica que del total de los 50 riesgos identificados, el 8% son inadmisibles, el 66% son inaceptables, 14% son tolerables y el 12% son aceptables.

Tabla 16. Matriz de riesgos posterior a la aplicación del SGCI

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3	(12) - (31) - (32) -		(15) -	(13) - (14) - (16) - (17) - (18) - (19) - (20) - (21) - (22) - (26) - (27) - (28) - (29) - (30) - (33) - (34) - (35) - (36) - (37) - (38) - (39) - (40) - (41) - (42) - (43) - (44) - (46) - (47) - (48) - (49) - (50) -	(23) - (24) - (25) - (45) -
Improbable	2	(4) - (5) - (11) -		(1) - (2) - (3) - (7) - (8) - (9) - (10) -	(6) -	
Raro	1					

Nota. Resultados del segundo análisis de riesgos realizado a la organización posterior a la implementación del SGCI.

En la *Tabla* 17, se identifica la distribución porcentual del escenario de riesgo en la organización del sector manufactura-textil, como se puede visualizar, posterior a la aplicación del SGCI se logró una distribución mucho más amplia.

Tabla 17. Distribución porcentual del escenario de riesgo en la organización posterior a la validación del SGCI

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	12,00	6
Tolerable	14,00	7
Inaceptable	66,00	33
Inadmisible	8,00	4

Nota. Resultado porcentual del escenario de riesgo en la organización posterior a la validación del SGCI. Fuente: Elaboración propia

Posterior a la implementación del SGCI, en la *Tabla* 18, se realiza la comparación de los dos escenarios de riesgos con el fin de verificar que la implementación del sistema de gestión de ciberseguridad industrial

propuesto en el presente proyecto de grado reduce en gran proporción la materialización de riesgos en el sector manufactura-textil.

Tabla 18. Comparación de los dos escenarios de riesgos

Probabilidad	valor	Consecuencia				
		Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					(19) - (26) - (41) - (42) - (43) - (45) - (49) - (50) -
Probable	4		(4) - (5) - (11) - (12) - (31) - (32) - (38) -	(44) -	(1) - (2) - (3) - (8) -	(6) - (7) - (9) - (10) - (13) - (14) - (15) - (16) - (17) - (18) - (20) - (21) - (22) - (23) - (24) - (25) - (27) - (28) - (29) - (30) - (33) - (34) - (35) - (36) - (37) - (39) - (40) - (46) - (47) - (48) -
Posible	3					
Improbable	2					
Raro	1					

Probabilidad	valor	Consecuencia				
		Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3	(12) - (31) - (32) -		(15) -	(13) - (14) - (16) - (17) - (18) - (19) - (20) - (21) - (22) - (26) - (27) - (28) - (29) - (30) - (33) - (34) - (35) - (36) - (37) - (38) - (39) - (40) - (41) - (42) - (43) - (44) - (46) - (47) - (48) - (49) - (50) -	(23) - (24) - (25) - (45) -
Improbable	2	(4) - (5) - (11) -		(1) - (2) - (3) - (7) - (8) - (9) - (10) -	(6) -	
Raro	1					

Nota. Comparación de los dos escenarios de riesgos, el de la izquierda corresponde al resultado antes de implementar el SGCI, el de la derecha corresponde al resultado luego de la implementación del SGCI. Fuente: Elaboración propia

Como se evidencia en la *Tabla* 19, con la validación del SGCI se lograron reducir los riesgos de la organización del sector manufactura-textil de la siguiente manera:

- Los riesgos inadmisibles se redujeron del 92,86% al 8%.
- Los riesgos inaceptables aumentaron del 7,14% al 66%.
- Los riesgos tolerables aumentaron del 0% al 14%.
- Los riesgos aceptables aumentaron del 0% al 12%.

El aumento de los riesgos inaceptables, tolerables y aceptables corresponde a que se logró reducir en gran proporción los riesgos inadmisibles, estos a su vez se lograron reducir en riesgos tolerables y estos en riesgos aceptables, este es un indicador positivo en el presente escenario de riesgo.

Tabla 19. Comparación de la distribución porcentual del escenario de riesgo final.

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	0,00	0
Tolerable	0,00	0
Inaceptable	7,14	2
Inadmisible	92,86	26

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	12,00	6
Tolerable	14,00	7
Inaceptable	66,00	33
Inadmisible	8,00	4

Nota. Resultado porcentual del escenario de riesgo en la organización antes y luego de la validación del SGCI. Fuente: Elaboración propia

Cómo se logró comprobar, la validación del sistema de gestión de ciberseguridad industrial propuesto en el presente trabajo representa una herramienta para fortalecer la protección de los entornos industriales contra las crecientes amenazas cibernéticas. Se identificó que este enfoque estratégico demuestra su eficacia a través de la mitigación de los riesgos de ciberseguridad en los entornos industriales del sector manufactura-textil. Con la implementación del SGCI, se fortalecieron cada uno de los dominios propuestos dentro del modelo creado, adicionalmente, se redujo la probabilidad de interrupciones no deseadas y se fortaleció la

continuidad de las mismas. Se aumentó la concientización y el compromiso de los empleados con prácticas de seguridad sólidas, lo que ha llevado a una disminución significativa en las brechas de seguridad causadas por errores humanos. El SGCI ha permitido la identificación temprana y la respuesta rápida a amenazas y ataques cibernéticos, minimizando el impacto en los activos críticos y la reputación de la organización. La capacidad para gestionar incidentes de seguridad se ha fortalecido notablemente y puede seguir mejorando durante el sostenimiento del SGCI.

CONCLUSIONES

El resultado de este proyecto representó un nuevo modelo en la protección de las infraestructuras industriales en el sector manufactura-textil, en un entorno cada vez más interconectado donde la ciberseguridad se ha convertido en una prioridad ineludible. El modelo proporcionó un marco sólido y efectivo para gestionar y mitigar los riesgos de seguridad informática en las tecnologías de la operación en el sector, preservando y fortaleciendo la disponibilidad, la integridad y la confidencialidad en estos ambientes industriales.

La caracterización de los estándares y sistemas de gestión de ciberseguridad a través del análisis de relevancia permitieron no solo una comprensión profunda de cada uno de los marcos de referencia, sino que también han permitido identificar cuáles de ellos estaban en sintonía o podrían ser alineados con la estrategia propuesta en el modelo de gestión de ciberseguridad industrial enfocado en el ambiente de las TO para el sector manufactura-textil. Este análisis permitió concluir que de los estándares más ajustados al modelo propuesto fueron los marcos ISO 27001:27002, IEC 62443 y NIST 800-82. Adicionalmente, con el resultado del análisis de relevancia, se lograron seleccionar las mejores prácticas para la creación del modelo de ciberseguridad industrial.

La construcción del modelo de gestión de ciberseguridad industrial contribuyó significativamente con la protección de los activos y la mitigación de los riesgos de seguridad cibernética en el entorno industrial. A lo largo de esta construcción, se definieron 7 dominios representados en los pilares fundamentales sobre los cuales se apoyó el modelo de gestión. Estos dominios encapsularon una estrategia integral de gestión de ciberseguridad, abarcando desde el contexto de la organización y el compromiso de la alta dirección hasta la segmentación de redes, gestión de riesgos y cultura de ciberseguridad. Cada dominio fue respaldado por las mejores prácticas de los marcos de ciberseguridad investigados y permitieron mitigar los riesgos de seguridad en la industria manufactura-textil.

La validación del sistema de gestión de ciberseguridad industrial, enfocado en las TO a través del caso de estudio en una empresa del sector manufactura-textil, permitió comprobar la eficacia del modelo propuesto. Durante este proceso, se logró concluir que la correcta implementación de cada uno de los dominios establecidos en el modelo, permitieron mitigar los riesgos de ciberseguridad industrial en la organización como se logró identificar en las *Tablas* 18 y 19, logrando como resultado una organización mejor preparada para afrontar los desafíos actuales y futuros a nivel de ciberseguridad industrial.

Durante la ejecución del dominio 3 se logró modificar el organigrama de la organización debido a que antes de la aplicación del SGCI la coordinación de seguridad se encontraba dentro de la jefatura de plataforma informática. Gracias a la validación del SGCI se logró separar la coordinación al mismo nivel de las jefaturas. Este cambio permitió empoderar aún más al proceso de ciberseguridad lo cual se representa en una mejor estructura con énfasis en la gestión de incidentes y políticas a nivel industrial globales para la organización.

El dominio 7, correspondiente a la promoción de cultura en ciberseguridad, logró aumentar la concientización de los empleados reduciendo la exposición de credenciales gracias al desarrollo de la campaña anti-phising donde se logró reducir de 63% a un 13% el porcentaje de exposición de credenciales.

ANEXOS

A. Anexo 01 - Dominio 1 - Contexto de la organización
B. Anexo 02 - Dominio 2 - Inventario de activos industriales
C. Anexo 03 - Dominio 2 - Inventario de amenazas
D. Anexo 04 - Dominio 2 - Inventario de vulnerabilidades
E. Anexo 05 - Dominio 2 - Inventario de controles existentes
F. Anexo 06 - Dominio 2 - Gestión de riesgo
G. Anexo 07 - Dominio 3 - Estrategia de ciberseguridad industrial
H. Anexo 08 - Dominio 1 - Contexto de la organización
I. Anexo 09 - Dominio 2 - Inventario de activos industriales
J. Anexo 10 - Dominio 2 - Inventario de amenazas
K. Anexo 11 - Dominio 2 - Inventario de vulnerabilidades
L. Anexo 12 - Dominio 2 - Inventario de controles existentes
M. Anexo 13 - Dominio 2 - Gestión de riesgo
N. Anexo 14 - Dominio 3 - Estrategia de ciberseguridad industrial
O. Anexo 15 - Dominio 2 - Gestión de riesgo con SGCI

REFERENCIAS BIBLIOGRÁFICAS

[1] El centro de ciberseguridad industrial y la estrategia de ciberseguridad nacional de España, «SOPORTANDO, APOYANDO Y DESARROLLANDO LA CIBERSEGURIDAD NACIONAL DESDE LA CIBERSEGURIDAD INDUSTRIAL», 2014.

[2] C. D. C. Industrial, *Guía para la construcción de un SGCI*. 2015. [En línea]. Disponible en: www.cci-es.org

[3] N. López, «¿Está cerca la Industria 4.0 en Colombia?», LA REPÚBLICA. Accedido: 30 de abril de 2022. [En línea]. Disponible en: https://www.larepublica.co/internet-economy/esta-cerca-la-industria-40-en-colombia-2600242

[4] Fortinet, «Causes_and_Consequences_of_TI_Boom.pdf», *India Review*, 2019.

[5] C. B. Espinosa Garrido y L. Rosales Roldan, «Marco de Referencia de Ciberseguridad para Dispositivos de IoT Usando la Tecnología de IDS», en *Memorias de la Décima Segunda Conferencia Iberoamericana de Complejidad, Informática y Cibernética: CICIC 2022*, 2022, pp. 210-215. doi: 10.54808/cicic2022.01.210.

[6] A. Castillo y A. D. Thierer, «Projecting the Growth and Economic Impact of the Internet of Things», *SSRN Electronic Journal*, 2015, doi: 10.2139/ssrn.2618794.

[7] Fortinet, «2021 State of Operational Technology and Cybersecurity Report», 2021. Accedido: 2 de mayo de 2022. [En línea]. Disponible en: https://www.fortinet.com/resources-campaign/operational-technology/2021-the-state-of-operational-technology-and-cybersecurity

[8] «Industrial Internet of Things (IIoT) Market Research Report: Market size, Industry outlook, Market Forecast, Demand Analysis, Market Share, Market Report 2021-2026». Accedido: 29 de noviembre de 2022. [En línea]. Disponible en: https://www.industryarc.com/Report/7385/industrial-internet-of-things-(IIoT)-market-report.html

[9] Ministerio del Interior y Secretaría de estado de Seguridad Española, «Guía sobre controles de seguridad en sistemas TO», España, 2020. [En línea]. Disponible en: https://www.ismsforum.es/ficheros/descargas/maquetaguiaotv101621955967.pdf

[10] C. Bernstein, «What is the Presidential Policy Directive 21 (PPD-21)? » Accedido: 9 de mayo de 2022. [En línea]. Disponible en: https://www.techtarget.com/whatis/definition/Presidential-Policy-Directive-21-PPD-21

[11] A. Amirault y I. Ferreira dos Santos, «Securing industrial networks: What is ISA/IEC 62443?», 2021, Accedido: 9 de mayo de 2022. [En línea]. Disponible en: https://blogs.cisco.com/security/securing-industrial-networks-what-is-isa-iec-62443

[12] J. Pan y Z. Yang, «Cybersecurity challenges and opportunities in the new “edge computing + iot” world», *SDN-NFVSec 2018 - Proceedings of the 2018 ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization, Co-located with CODASPY 2018*, vol. 2018-Janua, pp. 29-32, 2018, doi: 10.1145/3180465.3180470.

[13] A. T. Chatfield y C. G. Reddick, «A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government», *Gov Inf Q*, vol. 36, n.º 2, pp. 346-357, 2019, doi: 10.1016/j.giq.2018.09.007.

[14] S. N. Matheu-García, J. L. Hernández-Ramos, A. F. Skarmeta, y G. Baldini, «Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices», *Comput Stand Interfaces*, vol. 62, n.º November 2018, pp. 64-83, 2019, doi: 10.1016/j.csi.2018.08.003.

[15] A. Calder, *NIST Cybersecurity Framework: A Pocket Guide*. TI Governance Publishing, 2018. Accedido: 9 de mayo de 2022. [En línea]. Disponible en: https://www.itgovernanceusa.com/shop/product/nist-cybersecurity-framework-a-pocket-guide

[16] Centro de Ciberseguridad Industrial, «Ciberseguridad en la pirámide de automatización industrial», 2018. [En línea]. Disponible en: https://www.cci-es.org/documents/10694/304600/Guia+Bolsillo+-+Piramide+de+Automatizacion+Industrial.pdf/4d210379-b950-4d42-82fb-81a271113104

[17] MINTIC, «Gobierno nacional publica borrador del decreto de ciberseguridad para el país», 31 ENERO 2022. Accedido: 9 de septiembre de 2022. [En línea]. Disponible en: https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/198588:Gobierno-nacional-publica-borrador-del-decreto-de-ciberseguridad-para-el-pais

[18] J. Rebolledo, C. Duque, L. Á. López, y A. Velasco, «Perfil del sector manufacturero Colombiano Profile of Colombian manufacturing sector», 2013.

[19] O. Ynzunza, C., Izar, J.M., Bocarando, J., Aguilar, F., Larios, «El entorno de la industria 4.0: implicaciones y perspectivas futuras», *Conciencia tecnológica*, n.º 54, pp. 33-45, 2017, [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6405835&info=resumen&idioma=ENG%0Ahttps://dialnet.unirioja.es/servlet/articulo?codigo=6405835&info=resumen&idioma=SPA%0Ahttps://dialnet.unirioja.es/servlet/articulo?codigo=6405835%0Ahttps://www.redalyc.o

[20] N. Oliva *et al.*, *Redes de Comunicaciones Industriales*. Madrid: Universidad Nacional de educación a Distancia Madrid, 2013.

[21] R. Blanco Díaz, J. Fontodrona Francolí, y C. Poveda Martínez, «La industria 4.0: El estado de la cuestión», *Economía industrial*, n.º 406, pp. 151-164, 2017, Accedido: 2 de mayo de 2022. [En línea]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6343649#

[22] RedHat, «¿Qué es el Internet industrial de las cosas?», ¿Qué es el Internet industrial de las cosas? Accedido: 2 de mayo de 2022. [En línea]. Disponible en: https://www.redhat.com/es/topics/internet-of-things/what-is-iiot

[23] K. H. Niemann, «Differentiation of the TI security standard series ISO 27000 and IEC 62443», 2021, doi: https://doi.org/10.25968/opus-1973.

[24] C. Patricia, P. Arroyave, E. Superior De Guerra, y R. R. Prieto, «Lineamientos de ciberseguridad para mejorar la protección de los sistemas de control industrial. Caso de estudio: ISA INTERCOLOMBIA Maestría en Ciberseguridad y Ciberdefensa».

[25] M. R. Ospina Díaz, P. E. Sanabria Rangel, M. R. Ospina Díaz, y P. E. Sanabria Rangel, «Revista Criminalidad.», *Revista Criminalidad*, vol. 62, n.º 2, Dirección de Investigación Criminal, pp. 199-217, 2020. Accedido: 30 de abril de 2022. [En línea]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&nrm=iso&tlng=es

[26] M. R. Ospina Díaz y P. E. Sanabria Rangel, «Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia», *Revista Criminalidad*, vol. 62, n.º 2, pp. 199-217, 2020, Accedido: 9 de mayo de 2022. [En línea]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lng=en&nrm=iso&tlng=es

[27] J. Mario, A. Correa, L. Marín Ramírez, y J. Á. Salazar, «modelo C2M2 para la industria manufacturera del sector textil Identification of safety elements based on the C2M2 model for the textile industry», *Revista Colombiana de Computación*, vol. 20, n.º 2, pp. 56-67, 2019, doi: 10.29375/25392115-3722.

[28] C. F. Collado y P. Baptista, *Metodología de la investigación*. México DF: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V., 2014. [En línea]. Disponible en: https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

[29] M. Frayssinet Delgado, D. Esenarro, F. F. Juárez Regalado, y M. Díaz Reátegui, «Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations», *3C TIC: Cuadernos de desarrollo aplicados a las TIC*, vol. 10, n.º 2, pp. 123-141, 2021, doi: 10.17993/3ctic.2021.102.123-141.

[30] «Cybersecurity Frameworks», 2022. Accedido: 22 de abril de 2023. [En línea]. Disponible en: https://satoricyber.com/data-protect-guide/cybersecurity-frameworks/

[31] «STAR | CSA». Accedido: 22 de abril de 2023. [En línea]. Disponible en: https://cloudsecurityalliance.org/star/

[32] «HITRUST Alliance | Information Risk Management and Compliance». Accedido: 22 de abril de 2023. [En línea]. Disponible en: https://hitrustalliance.net/

[33] «NERC CIP | Tenable®». Accedido: 22 de abril de 2023. [En línea]. Disponible en: https://es-la.tenable.com/solutions/nerc-cip

[34] M. Benz y D. Chatterjee, «Calculated risk? A cybersecurity evaluation tool for SMEs», *Bus Horiz*, vol. 63, n.º 4, pp. 531-540, 2020, doi: 10.1016/j.bushor.2020.03.010.

[35] A. Mahn, J. Marron, S. Quinn, D. Topper, T. U. courtesy of Department of State with support from the Digital Connectivity, y C. Partnership, «Primeros pasos de NIST Marco de ciberseguridad: Guía de inicio rápido», *NIST*, 2021, doi: 10.6028/NIST.SP.1271es.

[36] TI Governance USA, «ISO 27001, the Information Security Standard | TI Governance USA». Accedido: 9 de mayo de 2022. [En línea]. Disponible en: https://www.itgovernanceusa.com/iso27001

[37] ISO, «ISO - ISO/IEC 27002:2013 - Information technology — Security techniques — Code of practice for information security controls». Accedido: 9 de mayo de 2022. [En línea]. Disponible en: https://www.iso.org/standard/54533.html

[38] ISA, «Quick Start Guide : Quick Start Guide : An Overview of ISASecure ® Certification», 2020, [En línea]. Disponible en: https://www.isasecure.org/en-US/Documents/0920-ISASecure-QuickStart-Guide-FINAL

[39] D. Ortiz García, «Ciberseguridad en la Industria 4.0 for dummies», Ciberseguridad en la Industria 4.0 for dummies. Accedido: 14 de octubre de 2023. [En línea]. Disponible en: https://trends.inycom.es/ciberseguridad-en-la-industria-4-0-for-dummies/

[40] A. : Alejandro y S. Lóndero, «“Arquitecturas de seguridad TO y protección mediante Deception”», 2021. Accedido: 2 de mayo de 2022. [En línea]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/138706/6/ascattonTFM1221memoria.pdf