Modelo para la ejecución de auditorías de seguridad en sistemas industriales SCADA usando buenas prácticas internacionales.

Dirlian Rony Caicedo Portilla

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2024

Modelo para la ejecución de auditorías de seguridad en sistemas industriales SCADA usando buenas prácticas internacionales.

Dirlian Rony Caicedo Portilla

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

PhD. Miguel Ángel Roldán Álvarez

Línea de Investigación:

Ciencias Computacionales

Grupo de Investigación:

Automática, electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2024

Dedicado:
A Dios el único que me abre los ojos del conocimiento.

Agradecimientos

A Dios,

A mi padre, por sus oraciones y voz de aliento para continuar siempre adelante.

A mi hermana, por apoyarme cada vez que lo necesité.

A todos mis familiares, amigos y compañeros que estuvieron atentos a este proceso y me motivaron para no desfallecer.

A los docentes del ITM, que aportaron de una u otra forma con el logro de la hazaña que representa este trabajo.

Resumen

El proyecto de grado está orientado a el diseño de un modelo para llevar a cabo auditorías de seguridad en sistemas industriales SCADA, siguiendo buenas prácticas internacionales. La creciente interconectividad y digitalización en entornos industriales han elevado la seguridad de los sistemas SCADA como una preocupación crítica para las organizaciones. El objetivo principal es proporcionar a las empresas un enfoque estructurado y eficiente para realizar auditorías de seguridad en sus sistemas SCADA, utilizando el Marco de Ciberseguridad del NIST (CSF) como referencia. El proceso propuesto abarca diversas etapas, desde la definición del alcance de la auditoría hasta la generación de recomendaciones para abordar riesgos identificados. Se destaca la importancia de la priorización de acciones correctivas, proporcionando plazos sugeridos para su implementación. Además, se subraya la necesidad de un enfoque proactivo en la gestión de la seguridad de los sistemas SCADA, fomentando la implementación de controles robustos y la mejora continua de la postura de seguridad. La contribución clave de este proyecto radica en la creación de un modelo práctico y adaptable a diferentes entornos industriales. Permitirá a las organizaciones evaluar y fortalecer la seguridad de sus sistemas SCADA, brindando una guía paso a paso para la realización de auditorías de seguridad y asegurando el cumplimiento de las buenas prácticas internacionales para la protección de los activos empresariales. En resumen, este proyecto propone un modelo integral que busca fortalecer la seguridad en entornos industriales cada vez más interconectados y digitalizados, al tiempo que garantiza el cumplimiento de estándares internacionales de ciberseguridad.

Palabras clave:

Auditoría de Seguridad, Buenas Prácticas, Normas Internacionales, Riesgos Técnicos, Sistemas Industriales SCADA.

Abstract

The undergraduate project focuses on designing a model for conducting security audits in industrial SCADA systems, adhering to international best practices. The increasing interconnectivity and digitization in industrial environments have elevated the security of SCADA systems as a critical concern for organizations. The main objective is to provide companies with a structured and efficient approach to perform security audits on their SCADA systems, using the NIST Cybersecurity Framework (CSF) as a reference. The proposed process spans various stages, from defining the scope of the audit to generating recommendations to address identified risks. Emphasis is placed on the prioritization of corrective actions, along with suggested timelines for implementation. Additionally, the need for a proactive approach in managing the security of SCADA systems is underscored, encouraging the implementation of robust controls and the continuous improvement of the security posture. The key contribution of this project lies in creating a practical and adaptable model for different industrial environments. It will enable organizations to assess and strengthen the security of their SCADA systems, providing a step-by-step guide for security audits and ensuring compliance with international best practices for protecting corporate assets. In summary, this project proposes a comprehensive model aimed at enhancing security in increasingly interconnected and digitized industrial settings while ensuring compliance with international cybersecurity standards.

Keywords:

Good Practices, International Standards, SCADA Industrial Systems, Security Audit, Technical Risks.

Índice general

Pág.

Índice de figuras

Pág.

Índice de tablas

Pág.

Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
SCADA	Sistema de Control y Adquisición de Datos (Supervisory Control And Data Acquisition, en inglés).
HMI	Interfaz Hombre-Máquina (Human-Machine Interface, en inglés).
PLC	Controlador Lógico Programable (Programmable Logic Controller, en inglés).
RTU	Unidad Terminal Remota (Remote Terminal Unit, en inglés).
MTU	Unidad Terminal Maestra (Master Terminal Unit, en inglés).
ISO	Organización Internacional de Normalización (International Organization for Standardization, en inglés).

Abreviatura	Término
NIST	Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology, en inglés).
CSF	Marco de Ciberseguridad (Cybersecurity Framework, en inglés).
COBIT	Control Objectives for Information and Related Technologies.
CIS	Centro para la Seguridad en Internet (Center for Internet Security, en inglés).
COSO	Comité de Organizaciones Patrocinadoras de la Comisión Treadway (Committee of Sponsoring Organizations of the Treadway Commission, en inglés).
OWASP	Proyecto de Seguridad de Aplicaciones Web de Open Web Application Security Project.
ISACA	Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association, en inglés).
ISA	Sociedad Internacional de Automatización (International Society of Automation, en inglés).
NERCP	Plan Nacional de Recuperación y Estabilización de Ciberespacio (National Cybersecurity and Communications Integration Center, en inglés).
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información (Information Technology Infrastructure Library, en inglés).

Introducción

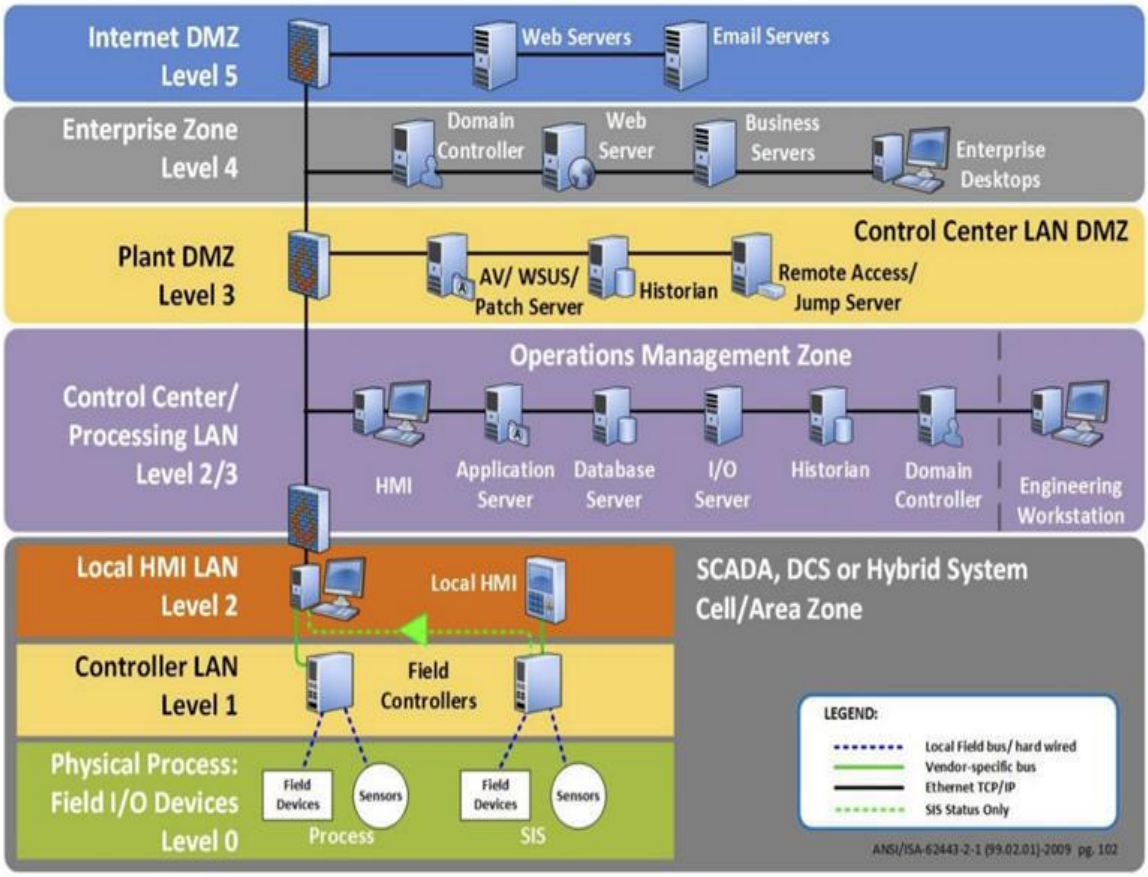
En los últimos tiempos, diversos sectores industriales, productivos y esenciales han vivido una transformación significativa con la automatización y digitalización de sus operaciones. Algunos se han alineado con la tendencia de la Industria 4.0, mientras que otros han adoptado estos cambios impulsados por la pandemia del coronavirus. La operación remota de máquinas ha permitido mejorar los servicios, fusionando las redes de Tecnologías de Información (IT) y Tecnologías de las Operaciones (OT). Esta integración facilita la automatización, el monitoreo eficiente y la gestión efectiva de sistemas [1].

No obstante, este progreso presenta desafíos, y uno de los peligros emergentes es la posibilidad de ataques cibernéticos. Cuando se habla de organizaciones con redes industriales, se hace referencia a sectores como el transporte, el petróleo, el gas natural, el agua potable, las aguas residuales, la eléctrica, la pulpa, el papel, la alimentación y las bebidas, así como la fabricación discreta (automotriz, aeroespacial y bienes duraderos). Las entidades utilizan sistemas como el control industrial (ICS), la supervisión y adquisición de datos (SCADA), el internet de las cosas industriales (IIOT) y los sensores inteligentes para proporcionar información sobre los procesos en tiempo real [1]

Históricamente, las redes industriales operaban de manera aislada, sin conexión a la red corporativa, y el acceso remoto se limitaba a través de módems estándar. No obstante, hoy en día la presencia una evolución rápida de la industria hacia la integración más estrecha de las tecnologías de la información (TI) y las redes industriales, también conocidas como entornos de tecnología operativa (OT). La arquitectura de estos entornos OT se caracteriza por una estructura jerárquica en capas, cada una con funciones específicas, como se ilustra en la (figura 1), brindando un marco robusto para la operación eficiente y segura de sistemas industriales avanzados [1].

Figura 1.

Estructura jerárquica en capas arquitectura de entornos OT.

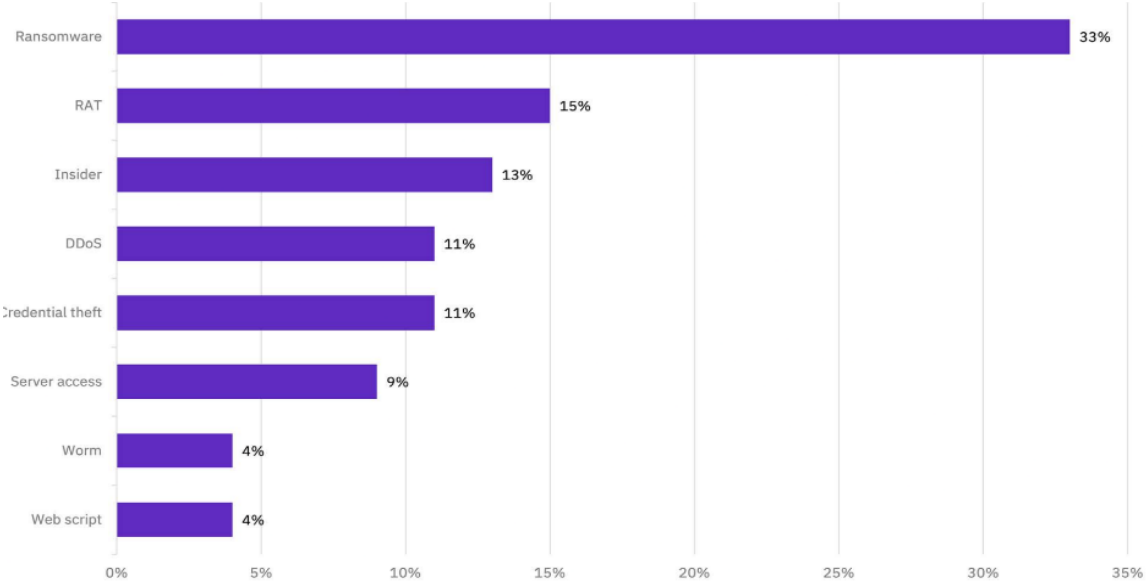


Nota. Esta figura explica cómo está conformada las capas de arquitectura de entornos OT adaptado de M. Bendel. "Índice de Inteligencia de Amenazas X-Force: el sector industrial se llevó la peor parte de los ciberataques en 2021, lo que agravó los problemas de las cadenas de suministro*". Fuente: Tomado de. [1].*

Según las estadísticas de ataques que se pueden evidenciar la figura 2, los ataques de ransomware constituyeron la mayoría de las amenazas más común para el entorno de trabajo temporal (OT); representaron el 33% de todos los ataques de OT en 2020. Algunas de las principales variedades de ransomware que se detectaron en ese año incluyeron EKANS, Nefilim, Medusa, PJX y Egregor. Estas variantes han demostrado ser particularmente dañinas y han sido responsables de una gran cantidad de accidentes en las redes industriales [1].

Figura 2.

Tipos de ataques contra OT 2020.



Nota. Esta figura explica el comportamiento de los ataques contra OT durante el año 2020 adaptado de M. Bendel. "Índice de Inteligencia de Amenazas X-Force: el sector industrial se llevó la peor parte de los ciberataques en 2021, lo que agravó los problemas de las cadenas de suministro". *Fuente: Tomado de. [1].*

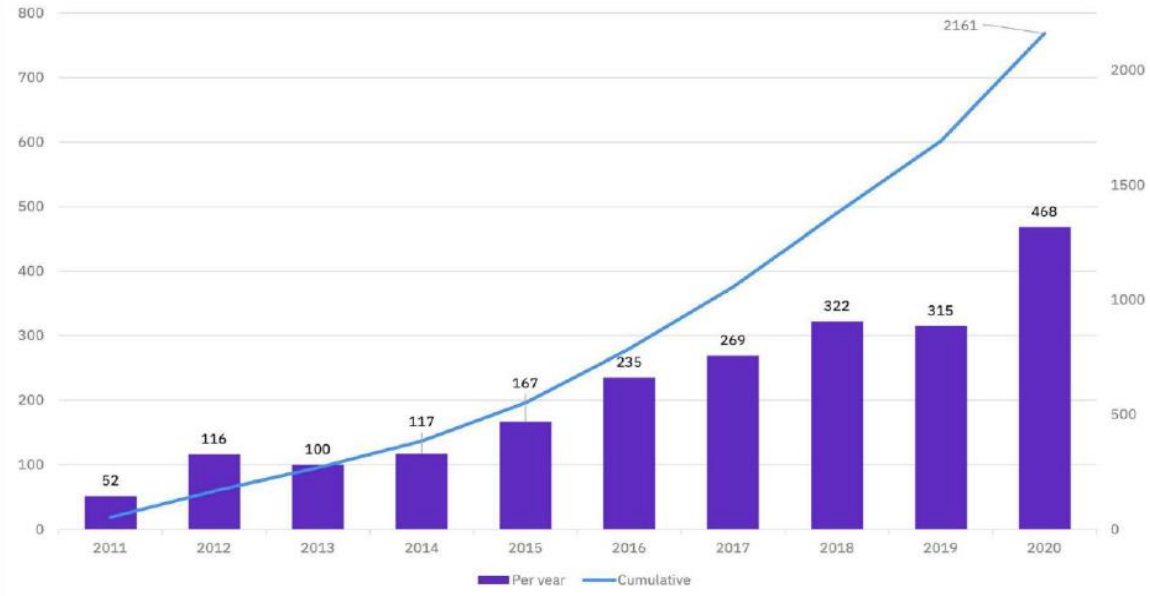
Por otro lado, se ha demostrado que los troyanos de acceso remoto (RAT) fueron el segundo tipo de ataque más frecuente contra entornos OT para 2020, representando el 15% de todos los riesgos registrados. Estos RAT permiten a los ciberdelincuentes acceder a dispositivos de manera remota, lo que les permite recopilar información de alta privacidad y manipular sistemas críticos. Durante ese tiempo, se detectaron RAT en redes OT como Trickbot, Adwind y jRAT, lo que destaca la complejidad y variedad de riesgos que enfrentan los entornos operativos. Esta tendencia enfatiza la necesidad de fortalecer las defensas contra troyanos de acceso remoto y la importancia de tomar medidas proactivas para prevenir y mitigar estos ataques en lugares de trabajo [1].

Los riesgos internos fueron un factor importante en el año 2020, representando el 13% de todos los riesgos relacionados con OT. El 60 % de este porcentaje estaba relacionado con personas internas con intenciones maliciosas, mientras que el 40 % restante estaba relacionado con negligencia del personal interno. Los riesgos internos maliciosos incluyeron acciones como empleados que conectaron a sitios web sospechosos con malware, así como otros que podrían haber vendido datos confidenciales de la empresa a sitios web de terceros. Este panorama destaca la importancia de implementar medidas de seguridad internas sólidas, así como la importancia de educar al personal sobre las amenazas internas y fomentar prácticas seguras en los entornos operativos para reducir los riesgos asociados con riesgos internos en entornos industriales críticos [1].

Además, los datos demuestran un continuo aumento en las vulnerabilidades de las plataformas ICS (Sistemas de Control Industrial), alcanzando un récord en 2020 después de una leve disminución en el año anterior. Este incremento se tradujo en un aumento significativo del 49% en las vulnerabilidades de ICS en comparación con el año precedente. La persistente tendencia al alza de estas vulnerabilidades plantea preocupaciones significativas, ya que intensifica el riesgo para los sistemas de tecnología operativa, aumentando la probabilidad de provocar efectos cinéticos destructivos en entornos industriales críticos. Estos hallazgos resaltan la necesidad apremiante de adoptar enfoques más rigurosos en materia de ciberseguridad para salvaguardar las plataformas ICS y mitigar los potenciales impactos adversos en la seguridad de los sistemas industriales [1].

Figura 3.

Vulnerabilidades de ICS, 2011- 2020.



Nota. Esta figura explica la tendencia de vulnerabilidad de ICS. *Fuente: Tomado de. [1].*

De acuerdo con la anterior figura, si bien es cierto que, las redes industriales y las infraestructuras críticas se asocian con frecuencia, estas no son las mismas cosas. La infraestructura crítica comprende sistemas y activos, ya sean físicos o virtuales, que son esenciales para el funcionamiento del país. Su incapacidad o destrucción puede afectar negativamente la seguridad, la economía nacional, la salud o la seguridad pública, o una combinación de estos aspectos. Un ejemplo de infraestructura crítica es el sector financiero, el cual no depende de una red industrial. Es importante hacer esta distinción, ya que, aunque a veces se usen términos similares, no son equivalentes. [1].

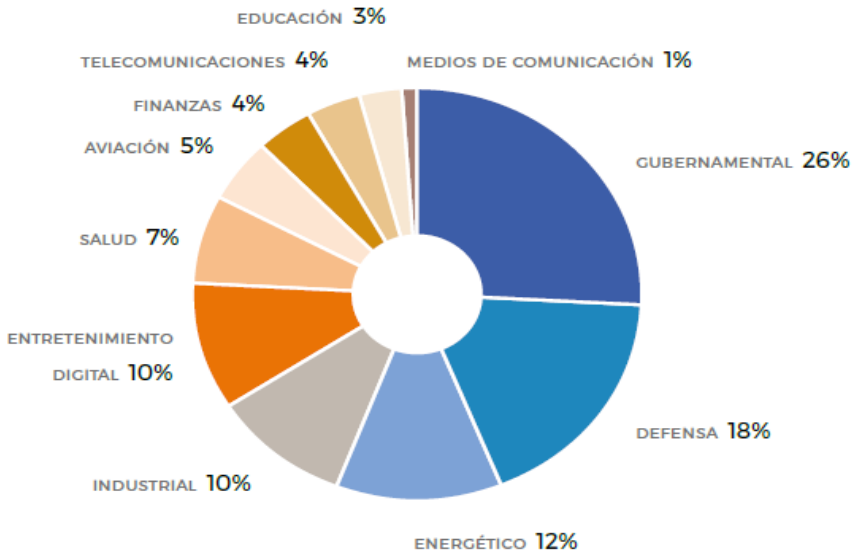
Es fundamental destacar la importancia de considerar las regulaciones destinadas a reducir los riesgos en entornos OT, especialmente para aquellas organizaciones que buscan establecer un marco de trabajo que cumpla con estándares y regulaciones específicas. Las

empresas con redes industriales y que operan en entornos OT deben estar completamente informadas sobre las normativas pertinentes que afectan su industria. Tomar medidas proactivas para cumplir con los requisitos de seguridad y ciberseguridad pertinentes se convierte en una prioridad ineludible. La aplicación de estos estándares garantiza la conformidad legal y mejora la resiliencia de los sistemas operativos, reduciendo su vulnerabilidad ante amenazas cibernéticas. Es fundamental estar al tanto de las regulaciones y actuar de acuerdo con ellas [1].

En cuanto a los sectores afectados los cuales se evidencia en la figura 4, el ámbito gubernamental resultó ser el más impactado por ataques cibernéticos, registrando una cantidad considerable de riesgos. Le sigue en la lista de afectaciones el sector de defensa, que también ha experimentado un número significativo de ataques, destacando la vulnerabilidad en este ámbito. Además, los sectores de energía, entretenimiento digital e industrial han sido blanco de una cantidad considerable de amenazas, evidenciando la amplia diversidad de objetivos para los ataques cibernéticos. Estos hallazgos subrayan la necesidad urgente de fortalecer las medidas de seguridad en estos sectores para mitigar los riesgos asociados a la ciberseguridad [2].

Figura 4.

Sectores y número de ocurrencias afectados por APT en 2020.



Nota. Esta figura explica la representación porcentual de sector y números de ocurrencia afectadas por APT durante el años 2020. Adaptado de A. S. Nikolaev, N. P. Pletneva y A. A. Pletnev, "Comparative analysis of the provisions of the standards gost r iso 19011-2012 (iso 19011: 2011) and iso 19011: 2018", *Fuente: tomado de [2].*

A raíz de la problemática descrita por sectores, la preocupación por la explotación de vulnerabilidades en plataformas importantes como Pulse Secure, CitrixNetscaler y F5 ha aumentado en la actualidad. Estas plataformas pueden permitir el acceso remoto no autorizado a sistemas industriales críticos. Un caso ejemplo ocurrió en 2021 cuando un atacante manipuló la dosificación de reactivos en una estación de tratamiento de agua en

Florida utilizando una configuración incorrecta del software de acceso remoto. Este caso demuestra la importancia de corregir los problemas de seguridad en infraestructuras importantes. Además, se emite una advertencia sobre el peligro que conlleva el uso continuo de Windows 7, especialmente después de la finalización de su soporte oficial, lo que aumenta la exposición a posibles peligros y resalta la importancia de tomar medidas para evitarlas [2].

En respuesta a la creciente conciencia de esta problemática, la Agencia de Ciberseguridad e Infraestructura (CISA) ha emitido una alerta urgente que destaca la necesidad de implementar medidas proactivas para salvaguardar los sistemas industriales en respuesta a cambios en su gestión. La advertencia enfatiza la necesidad de implementar un enfoque más sólido en seguridad cibernética para prevenir futuras amenazas y ataques. Además, se han descubierto campañas de phishing dirigidas específicamente a empresas industriales que utilizaban capturas de pantalla de la aplicación DIGSI de Siemens como cebo para propagar malware. Estas tácticas buscan infiltrarse y controlar los sistemas industriales, enfatizando la importancia de una mayor vigilancia y medidas defensivas para la ciberseguridad industrial [2].

Estos ataques tienen un impacto significativo en empresas industriales de diversos sectores, abarcando desde fabricación y petróleo hasta metalurgia, ingeniería, energía, construcción, minería y logística. La creciente cantidad de vulnerabilidades en sistemas de control industrial en los últimos años genera una seria preocupación por la exposición y riesgo que enfrentan estos sistemas. En consecuencia, es crucial implementar medidas sólidas para fortalecer la ciberseguridad en el ámbito industrial. En resumen, la adopción de acciones proactivas se vuelve imperativa para salvaguardar los sistemas industriales y reforzar la ciberseguridad, respondiendo así al aumento en la detección de vulnerabilidades en sistemas de control industrial [2].

Para la realización de este proyecto, se estableció como objetivo General: “Crear un modelo para la ejecución de auditorías de seguridad en sistemas industriales SCADA a través del uso de buenas prácticas internacionales para identificar y controlar riesgos técnicos y sus posibles impactos”. En este sentido el objetivo general se logró a través del cumplimiento de los siguientes objetivos específicos: generar un mapa de riesgos en los sistemas industriales, identificando amenazas y vulnerabilidades, caracterizar normas, estándares o buenas prácticas que estén asociadas al proceso de auditoría en seguridad para ser aplicados a los entornos industriales, proponer un plan de controles asociado a la reducción de los diferentes riesgos encontrados, con el fin de crear el modelo para la ejecución de auditorías y validar el modelo de seguridad para la ejecución de una auditoria sobre los sistemas industriales, considerando los riesgos y controles propuestos.

En este contexto, el documento incluye lo siguiente: documentación vigente de la literatura que respalda la investigación; un resumen de estudios previos y la recopilación de literatura relacionada; un enfoque metodológico detallado que guía la investigación; los hallazgos obtenidos durante su implementación; y las conclusiones.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

El documento actual compila información de diversos artículos de investigación, tesis de grado y otros documentos académicos, así como de repositorios de tesis de múltiples universidades. Estos documentos proponen proyectos sobre sistemas SCADA (Supervisión, Control y Adquisición de Datos) para monitorear y controlar el estado operativo de varios procesos, destacando su eficacia en la adquisición y supervisión de datos. Se han realizado numerosos estudios que analizan el impacto de los sistemas SCADA en diferentes actividades humanas.

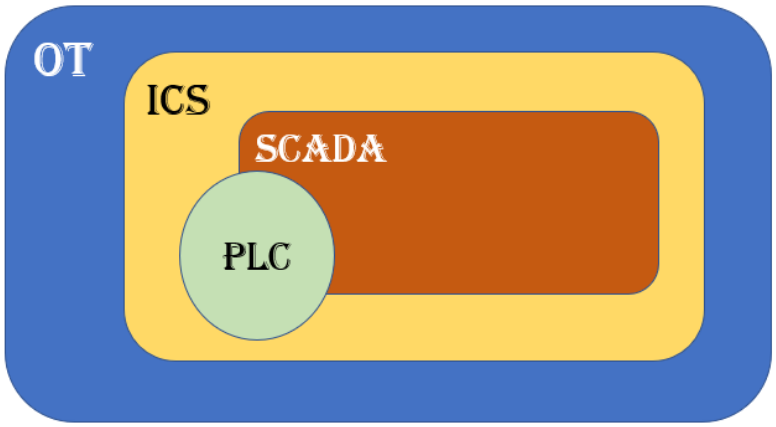
1.1.1 Tecnología Operativa

La tecnología operativa (OT) se refiere al hardware y software que se utiliza para supervisar y controlar los sistemas y procesos industriales. Se usa en una variedad de áreas, como la fabricación, la energía, el gas y el petróleo, el transporte, el agua y las aguas residuales. Los sistemas OT suelen ser autónomos y funcionan en redes separadas de las redes de TI. Esto se debe a que los sistemas OT deben funcionar con confiabilidad en tiempo real, independientemente de las fallas de las redes TI [3].

Los Sistemas de Control de Procesos (PCS) son fundamentales para administrar refinerías, plantas de energía y fábricas, así como los Sistemas de Control de Supervisión y Adquisición de Datos (SCADA) y los dispositivos de interfaz hombre-máquina (HMI) que brindan a los operadores la capacidad de interactuar con estos sistemas. La convergencia entre OT y TI, que busca aprovechar el análisis de datos e inteligencia artificial, es una tendencia en ascenso. Sin embargo, la vulnerabilidad de los sistemas OT a los ciberataques plantea nuevos desafíos para la seguridad. A pesar de estos inconvenientes, el uso de la tecnología operativa mejora la eficiencia, la productividad y la calidad. De esta manera la siguiente Figura 5 representa el entorno de un sistema de Tecnología Operativa (OT) que incluye un PLC [4].

Figura 5.

Interpretación de la tecnología operacional



Nota. Esta figura representa la interpretación de la tecnología operacional.

La imagen muestra una representación visual de la jerarquía de los sistemas de control industrial (ICS). El ICS es un término amplio que se refiere a cualquier sistema utilizado para monitorear y controlar operaciones industriales. Los SCADA y los PLC son dos tipos comunes de ICS.

1.1.2 Sistema de Control Industrial (ICS)

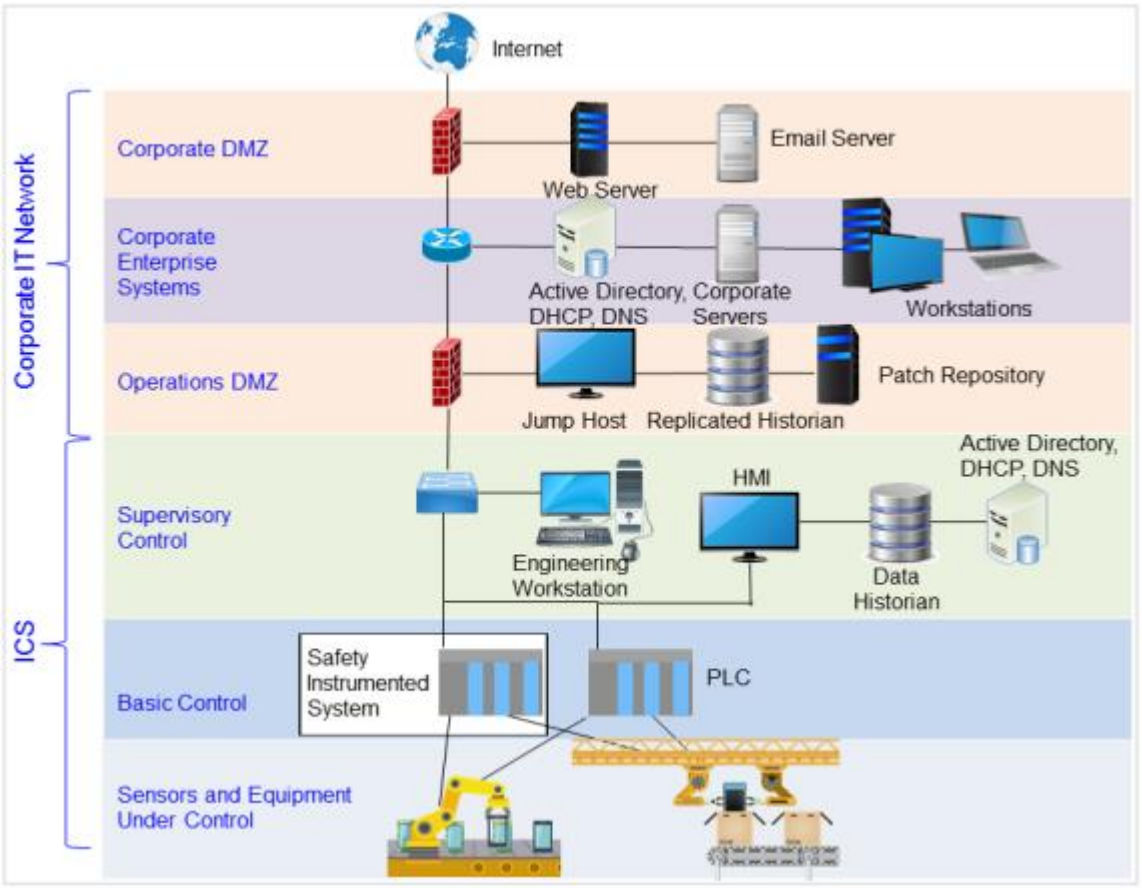
Los Sistemas de Control Industrial (ICS) son esenciales para muchas industrias porque brindan la capacidad de supervisar y controlar de manera confiable y eficiente los procesos industriales. Su trabajo principal es supervisar y controlar variables cruciales como temperatura, presión y flujo de materiales, entre otras, que son esenciales para el funcionamiento de numerosos procesos industriales. Estos sistemas incluyen actuadores, sensores, controladores lógicos programables (PLC) e interfaces hombre-máquina (HMI). Estos componentes trabajan juntos para permitir la recolección de datos del entorno industrial y la realización de acciones correctivas o preventivas para mantener la estabilidad y eficiencia de los procesos [5].

Su capacidad para monitorear y controlar variables cruciales aumenta la eficiencia operativa y gestiona los recursos industriales con gran precisión. Esta precisión es vital en áreas donde las desviaciones mínimas pueden tener un impacto significativo en la calidad del producto, la seguridad y los costos operativos. [5] Además, los ICS desempeñan un papel importante en el cambio hacia la Industria 4.0, donde la interconexión de sistemas y la integración de tecnologías emergentes como el Internet de las cosas (IoT) y el análisis de datos están redefiniendo los paradigmas de producción. Los ICS abren nuevas oportunidades para la optimización continua, el mantenimiento predictivo y el análisis de grandes cantidades de datos en tiempo real. Lo anterior es descrito en la figura 6.

La importancia de los ICS radica en su capacidad para garantizar el funcionamiento óptimo de procesos industriales cruciales en una variedad de industrias, como la fabricación, el petróleo y el gas, así como el transporte [6]. Su papel fundamental en la supervisión y control de variables clave mejora la eficiencia operativa de las industrias y promueve la seguridad y la confiabilidad de los procesos, lo que es esencial para la continuidad y el éxito de las operaciones industriales.

Figura 6.

ICS y arquitectura de red de TI corporativa



Nota. Esta figura representa ICS y arquitectura de red de TI corporativa. COSO, ERM . *Fuente: tomado de [5].*

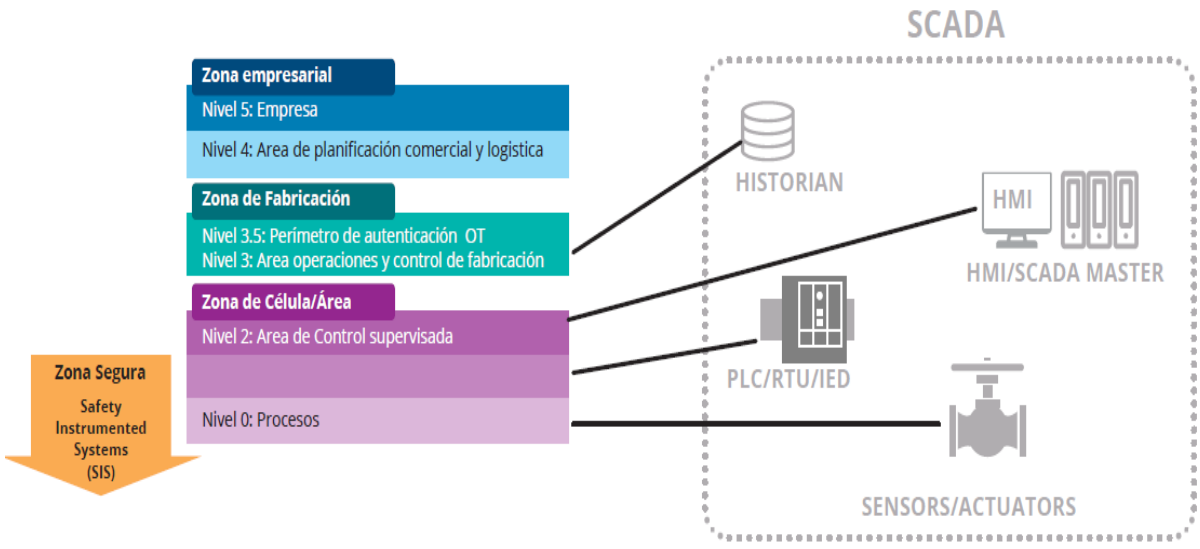
La imagen muestra una representación visual de la jerarquía de los sistemas de control industrial (ICS). El ICS es un término amplio que se refiere a cualquier sistema utilizado para monitorear y controlar operaciones industriales. Los SCADA y los PLCs son dos tipos comunes de ICS.

1.1.3 Sistemas SCADA

La mayoría de los procesos industriales y una gran cantidad de tareas cotidianas en la sociedad dependen de sistemas de monitorización y control en tiempo real. Sin embargo, una gran cantidad de ciudadanos no conocen estas tareas y sistemas. Se trata de dispositivos que se utilizan para realizar una variedad de tareas, como administrar el aire acondicionado o el sistema de calefacción de un edificio y distribuir energía eléctrica a nivel nacional. Los sistemas de control y monitorización SCADA son los más utilizados. El control de supervisión y adquisición de datos se conoce como SCADA [7].

Figura 7.

Diagrama Básico de un Sistema SCADA.



Nota. La figura representa la estructura básica del sistema SCADA. *Fuente: tomado de* [8]**.**

La imagen representa una estructura jerárquica de un sistema de control y automatización industrial, destacando la segregación de funciones en diferentes zonas y niveles. Este modelo asegura que las operaciones de negocio y fabricación se gestionen eficientemente, con medidas de seguridad adecuadas en cada nivel. La integración de sistemas como SCADA permite una monitorización y control efectivos, asegurando que los procesos industriales sean seguros, eficientes y bien coordinados.

1.1.4 Componentes de un sistema SCADA

Los sistemas SCADA (Supervisory Control And Data Acquisition) están compuestos por numerosos elementos que trabajan en conjunto para monitorear y controlar procesos industriales de forma eficiente. Los sistemas SCADA (Supervisión, Control y Adquisición de Datos) están compuestos por una serie de componentes importantes que ayudan a

monitorear y controlar de manera efectiva los procesos industriales [9]. Las Unidades de Terminal Remoto (RTU), que sirven como punto de contacto directo con los sensores y actuadores en el campo, son una de estas partes. Las RTU procesan las señales analógicas o digitales del entorno físico y las transmiten al centro de control a través de una red de comunicaciones, ya sea inalámbrica o cableada. El servidor maestro en el centro de control es responsable de recibir y procesar estos datos, lo que permite su visualización y análisis en tiempo real a través del software de supervisión y control SCADA [1].

El monitoreo en tiempo real de procesos y equipos, la capacidad de controlar los actuadores para ajustar dichos procesos y la generación de alarmas en caso de eventos anormales o condiciones fuera de rango son algunas de las funciones clave que demuestran la funcionalidad operativa de los sistemas SCADA. Además, el análisis de tendencias permite identificar patrones en los datos históricos para optimizar el rendimiento y predecir posibles fallas, lo que facilita la toma de decisiones informadas. Además, componentes sofisticados como IEDs, firewalls para protección cibernética y estándares de interoperabilidad como OPC y ODBC mejoran la funcionalidad y la seguridad del sistema. Las necesidades específicas de cada operación industrial también requieren aplicaciones específicas que ofrecen capacidades avanzadas de gestión de alarmas y análisis de datos. Estos componentes incluyen (Tabla 1):

Tabla 1.

Componenntes SCADA

Componente	Descripción
MI (Interfaz Hombre-Máquina)	Facilita la interacción entre el operario y la máquina al mostrar datos del proceso y permitir el control mediante una pantalla táctil.
Sistema de Supervisión (MTU)	Recopila datos del proceso, envía instrucciones según los valores actuales de las variables, almacena y procesa datos para su acceso por otros dispositivos.
Unidades Terminales Remotas (RTU)	Microprocesadores que reciben señales de acciones específicas, las transmiten de forma remota y se conectan a sensores para convertir señales en datos digitales.
PLC (Controlador Lógico Programable)	Dispositivos versátiles y configurables, utilizados para controlar acciones específicas en el proceso.
Red o sistema de comunicación	Establece la conectividad entre la Unidad Terminal Maestra (MTU), las Unidades Terminales Remotas (RTU) y los Controladores Lógicos Programables (PLC) a través de conexiones por módem, Ethernet, Wifi o fibra óptica.
Sensores	Detectan magnitudes físicas o químicas y las convierten en señales eléctricas para su procesamiento.
Actuadores	Dispositivos mecánicos que realizan acciones o generan movimiento en respuesta a las instrucciones del MTU o PLC.

Nota. Esta tabla explica cómo están conformado los componentes SCADAS. Adaptado de E. Pérez-López, "*Los sistemas SCADA en la automatización industrial", Fuente: tomado de [8].*

La tabla anterior proporciona una visión clara de los componentes clave en un sistema de automatización industrial, describiendo sus funciones y la interconexión entre ellos. La integración efectiva de estos componentes permite la supervisión y control eficientes de los procesos industriales, mejorando la productividad y seguridad. El HMI facilita la interacción humana, mientras que el MTU coordina el control y supervisión general. Los RTU y PLC realizan tareas específicas y se comunican a través de una red robusta. Los sensores y actuadores, por su parte, interactúan directamente con el entorno físico, ejecutando las instrucciones recibidas y proporcionando datos esenciales para el control del sistema.

Por otra parte los sistemas de control y adquisición de datos industriales (SCADA) son componentes esenciales en la operación de diversas industrias, controlando procesos críticos como la distribución de energía, el tratamiento de agua y el transporte de petróleo y gas. La complejidad y diversidad de los sistemas SCADA, junto con la creciente sofisticación de las amenazas cibernéticas, hacen imperativo considerar una amplia gama de elementos en las auditorías de seguridad para garantizar una protección integral [10].

Si bien la auditoría de seguridad SCADA debe centrarse en los componentes principales del sistema, como dispositivos de interfaz de campo (IEDs), redes de comunicación, servidor central, software SCADA e HMI, es fundamental considerar elementos adicionales que pueden afectar significativamente la postura de seguridad general tales como:

1. Dispositivos de Interfaz de Campo (IEDs):

- Evaluación de la seguridad de los IEDs: Analizar las medidas de seguridad implementadas en los IEDs, incluyendo autenticación, integridad de datos y protección contra ataques DoS.
- Verificación de las actualizaciones de firmware: Asegurar que los IEDs estén ejecutando la última versión del firmware para minimizar las vulnerabilidades conocidas.
- Validación de las configuraciones de seguridad: Revisar y validar las configuraciones de seguridad de los IEDs para garantizar que cumplan con las prácticas recomendadas.

2. Firewalls:

- Implementación de firewalls adecuados: Evaluar la presencia y efectividad de los firewalls en las redes SCADA, asegurando que brinden protección adecuada contra accesos no autorizados y tráfico malicioso.
- Configuración y gestión de firewalls: Revisar y optimizar la configuración de los firewalls para garantizar que solo se permita el tráfico legítimo y se bloqueen las amenazas potenciales.
- Monitoreo y registro de actividades: Implementar mecanismos de monitoreo y registro para las actividades del firewall, permitiendo detectar y responder a intentos de intrusión de manera oportuna.

3. OPC (OLE for Process Control):

- Análisis de la seguridad de las configuraciones OPC: Revisar las configuraciones de los servidores y clientes OPC para garantizar que solo usuarios autorizados puedan acceder a los datos y que se implementen mecanismos de autenticación y cifrado adecuados.
- Validación de las conexiones OPC: Verificar que las conexiones OPC estén restringidas a las redes y dispositivos necesarios, minimizando la exposición a ataques potenciales.
- Monitoreo y registro de las comunicaciones OPC: Implementar mecanismos de monitoreo y registro para las comunicaciones OPC, permitiendo detectar y analizar comportamientos anormales o intentos de intrusión.

4. ODBC (Open Database Connectivity):

- Evaluación de la seguridad de las conexiones ODBC: Revisar las configuraciones de las conexiones ODBC para garantizar que solo usuarios y aplicaciones autorizadas puedan acceder a las bases de datos.
- Implementación de mecanismos de autenticación y control de acceso: Asegurar que las conexiones ODBC se autentiquen mediante mecanismos robustos y que se implementen controles de acceso granular para limitar el acceso a los datos.
- Cifrado de las comunicaciones ODBC: Implementar el cifrado de las comunicaciones ODBC para proteger la confidencialidad e integridad de los datos sensibles.

5. Aplicaciones de Terceros:

- Evaluación de la seguridad de las aplicaciones: Analizar la seguridad de las aplicaciones de terceros integradas con el sistema SCADA, identificando posibles vulnerabilidades y riesgos de seguridad.
- Validación de las actualizaciones de las aplicaciones: Asegurar que las aplicaciones de terceros estén actualizadas con los últimos parches de seguridad para minimizar las vulnerabilidades conocidas.
- Control de accesos y permisos de las aplicaciones: Restringir el acceso a las aplicaciones de terceros solo a usuarios y sistemas autorizados, y limitar los permisos otorgados para minimizar el riesgo de ataques.

Por lo tanto hay que enfatizar que una auditoría de seguridad SCADA completa y efectiva, debe ir más allá de los componentes básicos del sistema y considerar una amplia gama de elementos que pueden afectar significativamente la postura de seguridad general. La evaluación de la seguridad de los IEDs, firewalls, OPC, ODBC y aplicaciones de terceros es fundamental para identificar y mitigar riesgos potenciales que podrían comprometer la integridad y disponibilidad de los sistemas SCADA. Además, es importante recordar que el alcance específico de la auditoría de seguridad SCADA puede variar según las necesidades de cada organización, los recursos disponibles y los riesgos potenciales identificados.

1.1.5 Auditoria

Las auditorías de ICS ya sean realizadas por auditores internos o externos con experiencia en seguridad de ICS, son esenciales para proteger los sistemas de control industrial de ciberataques y otras amenazas de seguridad. Este proceso sistemático comienza con una fase de planificación en la que los propietarios de ICS discuten los objetivos y alcances de la auditoría. Después de eso, se recopilan datos sobre las redes, la arquitectura y los componentes del sistema. Luego, se realiza una evaluación de riesgos para identificar amenazas, vulnerabilidades y efectos potenciales. Posteriormente, se llevan a cabo pruebas, como escaneos de vulnerabilidades y análisis de registros, para garantizar que se han identificado los riesgos [11].

Al mismo tiempo hay que destacar que las auditorías de ICS tienen muchos beneficios., en primer lugar, ayudan a mejorar la seguridad al identificar y corregir fallas que podrían ser explotadas por ciberataques, lo que ayuda a proteger la integridad y confidencialidad de los sistemas y datos industriales. Además, estas auditorías reducen el riesgo de interrupciones comerciales y pérdidas financieras al evitar riesgos de seguridad que podrían afectar la operatividad y la productividad. Por último, pero no menos importante, las auditorías de ICS son cruciales para el cumplimiento de normas y regulaciones de seguridad, lo que garantiza que las organizaciones cumplan con estándares reconocidos y minimicen el riesgo de sanciones legales o pérdida de reputación [12].

1.1.6 Tipos de auditorías

Existen diversas teorías y enfoques para realizar auditorías, cada uno con características y objetivos específicos. Uno de los enfoques más comunes es el basado en riesgos, que se centra en identificar y evaluar los riesgos potenciales que enfrenta una organización y en priorizar la asignación de recursos de auditoría en función de estos riesgos. Este método busca asegurar que los recursos se utilicen de manera efectiva para abordar los riesgos más significativos, maximizando así el impacto de la auditoría en la mejora de la gestión de riesgos y en el cumplimiento de los objetivos [11].

Además del enfoque basado en riesgos, también se encuentran teorías como el enfoque basado en procesos, que se centra en comprender y evaluar los procesos clave de una organización para encontrar áreas de mejora y eficiencia operativa. Otros enfoques incluyen la auditoría de cumplimiento, que se centra en verificar el cumplimiento de normas y regulaciones, y la auditoría operativa, que se centra en valorar la eficacia de los procesos y controles internos [11].

1.1.7 La auditoría de seguridad informática

La auditoría de seguridad informática se centra en la evaluación de riesgos y controles, similar a otras formas de auditoría, pero con un enfoque específico en la seguridad de los sistemas y datos digitales. Esta auditoría implica una evaluación sistemática de sistemas y procesos, la identificación de vulnerabilidades y riesgos, y la emisión de recomendaciones para mitigar estos riesgos. A diferencia de otras auditorías, su objetivo principal es proteger

la confidencialidad, integridad y disponibilidad de la información digital, además de prevenir ciberataques y brechas de seguridad. Esto incluye la evaluación de controles de acceso, la protección de datos, la gestión de identidades y contraseñas, y el análisis de vulnerabilidades en redes y sistemas [13].

1.1.8 Seguridad de la Información

La auditoría de seguridad informática se alinea con otros tipos de auditoría en su enfoque en la evaluación de riesgos y controles, pero se destaca por centrarse exclusivamente en la protección de los sistemas y datos digitales. Incluye una evaluación sistemática de los sistemas y procesos, identificando vulnerabilidades y riesgos, y luego ofrece sugerencias para reducirlos. No obstante, su enfoque distintivo se centra en proteger la confidencialidad, integridad y disponibilidad de la información digital, así como en la prevención activa de ciberataques y brechas de seguridad [14]. Esto la distingue como un campo porque requiere una evaluación exhaustiva de controles de acceso, protección de datos, gestión de identidades y contraseñas, y análisis de vulnerabilidades en redes y sistemas.

1.1.9 Seguridad Informática

La auditoría de seguridad informática se asemeja a otros tipos de auditoría en su enfoque en la evaluación de riesgos y controles. No obstante, se destaca por su enfoque exclusivo en la protección de los sistemas y datos digitales. Incluye una evaluación sistemática de los sistemas y procesos para encontrar vulnerabilidades y riesgos, y luego propone soluciones para abordarlos. Sin embargo, su enfoque distintivo se centra en proteger la confidencialidad, integridad y disponibilidad de la información digital, así como en la prevención activa de ciberataques y brechas de seguridad. Esto la distingue como una disciplina porque requiere una evaluación exhaustiva de controles de acceso, protección de datos, gestión de identidades y contraseñas y análisis de vulnerabilidades en redes y sistemas [15].

1.1.10 Ciberseguridad

Al igual que otras formas de auditoría, la auditoría de ciberseguridad se basa en teorías y métodos fundamentales para evaluar riesgos y controles. Sin embargo, su aplicación específica se centra en proteger los sistemas y datos digitales de las amenazas cibernéticas. El enfoque basado en riesgos, una teoría relevante en este contexto busca identificar y priorizar los riesgos potenciales para enfocar de manera efectiva los recursos de auditoría. Además, está relacionado con teorías de seguridad de la información, que incluyen principios como la confidencialidad, integridad y disponibilidad de los datos, así como la gestión de identidades y accesos [16].

1.1.11 Riesgos de Ciberseguridad

Para comprender los peligros de la ciberseguridad desde una perspectiva teórica, se pueden utilizar una variedad de marcos y modelos conceptuales. Uno de los métodos más populares es el modelo de la "tríada de la seguridad de la información", que se centra en la confidencialidad, integridad y disponibilidad de los datos como elementos clave de la seguridad de la información. Los accesos no autorizados pueden comprometer la confidencialidad de los datos, alterar su integridad o disminuir su disponibilidad, según este modelo [17].

1.1.12 Amenazas de Ciberseguridad

Las amenazas de ciberseguridad incluyen eventos, actores o circunstancias que pueden dañar los sistemas e información de una organización. Las diversas formas de este espectro de amenazas incluyen virus, hackers, ataques de phishing, ransomware y otros vectores maliciosos. Cada una de estas amenazas compromete la integridad, confidencialidad y disponibilidad de los datos de la empresa. Para diseñar e implementar estrategias de ciberseguridad que fortalezcan las defensas y minimicen los riesgos, es esencial reconocer y comprender estas amenazas. Para hacer frente a las amenazas de ciberseguridad, es necesario tomar medidas proactivas y actualizar constantemente las defensas [18].

1.1.13 Vulnerabilidades de Ciberseguridad

Las vulnerabilidades de ciberseguridad pueden entenderse desde una variedad de marcos teóricos. El modelo de "cadena de ataque" es un marco común que identifica varios puntos vulnerables en un sistema o red que podrían ser explotados por un atacante. Estos problemas pueden incluir fallas en el software, como errores de programación o falta de parches de seguridad, así como errores en la configuración de sistemas y redes, como contraseñas débiles o accesos no autorizados. Además, el modelo "CVE (Common Vulnerabilities and Exposures)" proporciona una taxonomía estándar para identificar y referenciar vulnerabilidades específicas en software y hardware. El análisis de riesgos es otro enfoque teórico importante que permite identificar y evaluar las vulnerabilidades en función [19].

1.1.14 Normas, marcos y buenas prácticas internacionales ampliamente reconocidas para la auditoría informática

Para garantizar la integridad y confidencialidad de los sistemas de información, son necesarios estándares, estándares y buenas prácticas para orientar y llevar a cabo el proceso de evaluación en el ámbito de la auditoría informática de ciberseguridad. Describe normas como ISO/IEC 27001, que es un marco de gestión de la seguridad de la información reconocido a nivel mundial. Además, el NIST Cybersecurity Framework, creado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU., proporciona directrices fundamentales sobre cómo mejorar la ciberseguridad de las organizaciones. Al establecer,

implementar, mantener y mejorar continuamente sus sistemas de gestión de la seguridad de la información, las organizaciones pueden mitigar de manera efectiva los riesgos cibernéticos mediante el uso de estos marcos. [16].

1.1.14.1 ISO 19011

El uso de un modelo de auditoría de seguridad para sistemas SCADA basado en la norma ISO 19011 aporta importantes beneficios en términos de seguridad y gestión de riesgos. Este método mejora la seguridad de los sistemas SCADA al identificar y reducir los peligros de seguridad. Además, este modelo de auditoría aumenta la confianza de todas las partes interesadas, incluidos administradores, usuarios y autoridades reguladoras, en la robustez de los sistemas SCADA al proporcionar una evaluación de seguridad independiente y objetiva [20].

Además, el modelo de auditoría basado en ISO 19011 mejora la gestión de riesgos y ayuda a las organizaciones a abordar los problemas de seguridad de manera proactiva. Este modelo no solo encuentra problemas, sino que también proporciona sugerencias sobre cómo mejorar la seguridad general de los sistemas SCADA. Además, la implementación de este modelo de auditoría ayuda a las organizaciones a promover una cultura de seguridad y cumplimiento normativo, lo que ayuda a cumplir con los requisitos normativos relacionados con la seguridad de la información [16].

1.1.14.2 GRC (Gobierno – Riesgo – Cumplimiento)

El marco de Gobernanza, Riesgo y Cumplimiento (GRC) es fundamental para las organizaciones en Colombia porque proporciona una estructura integral para gestionar los riesgos, cumplir con las regulaciones y alcanzar los objetivos estratégicos. Este enfoque holístico se basa en tres pilares: Gobernanza, que establece la estructura y las responsabilidades necesarias para una gestión eficiente; Riesgo, que implica la identificación, análisis y evaluación de amenazas potenciales; y Cumplimiento, que garantiza que la organización cumpla con todas las leyes, reglamentos y requisitos pertinentes [21].

1.1.15 ISO/IEC 27001

La norma ISO/IEC 27001, que es reconocida a nivel mundial, sirve como base para establecer los requisitos fundamentales para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). Esta normativa no es solo una guía; ofrece una estructura completa que capacita a las organizaciones para identificar, gestionar y reducir de manera efectiva los riesgos relacionados con la seguridad de la información. ISO/IEC 27001 fomenta la adopción de las mejores prácticas en el ámbito de la seguridad de la información, desde la minuciosa evaluación de vulnerabilidades hasta la aplicación de controles de seguridad robustos. Las organizaciones no solo fortalecen su postura de seguridad, sino que también demuestran un compromiso claro con estándares reconocidos a nivel global al seguir sus directrices [22].

1.1.16 NIST SP 800-53

El NIST SP 800-53, creado por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, ofrece un conjunto completo de instrucciones y controles de seguridad para sistemas de información y redes federales. Al proporcionar un marco detallado que aborda diversos aspectos de la seguridad informática, esta normativa ha adquirido un estatus fundamental para fortalecer la ciberseguridad en el ámbito gubernamental estadounidense. El NIST SP 800-53 es una herramienta vital para establecer medidas sólidas de seguridad en entornos federales, contribuyendo a la protección de la información sensible y la resiliencia de los sistemas, desde controles relacionados con el acceso y la autenticación hasta medidas específicas para la protección de datos y la gestión de riesgos [12].

1.1.17 CIS Controls

El Centro para la Seguridad en Internet (CIS) ha desarrollado un conjunto de controles de seguridad que se centran en acciones específicas y prácticas destinadas a proteger los sistemas de información contra las amenazas cibernéticas más comunes. Estos controles, cuidadosamente diseñados, abarcan desde la gestión de vulnerabilidades hasta la autenticación de usuarios, proporcionando un enfoque integral para fortalecer la postura de seguridad de las organizaciones [23].

La iniciativa del CIS responde a la necesidad de contar con directrices claras y efectivas en un entorno digital dinámico, proporcionando a las entidades un marco de referencia práctico y adaptable que se ajusta a la evolución constante del panorama de ciberseguridad. La contribución del CIS se convierte en un recurso valioso para la protección eficaz de la información y la preservación de la integridad de los sistemas de información en un mundo cada vez más interconectado.

1.1.18 NIST Cybersecurity Framework

Desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST), este marco de ciberseguridad se presenta como una guía esencial para que las organizaciones gestionen y reduzcan sus riesgos cibernéticos. Su enfoque se centra en la alineación de políticas, procedimientos y controles con las necesidades y objetivos específicos de cada entidad. Este marco, diseñado meticulosamente, no solo proporciona una estructura para evaluar y fortalecer las defensas cibernéticas, sino que también permite una adaptabilidad crucial a las cambiantes amenazas y exigencias del entorno digital. Al seguir este marco del NIST, las organizaciones pueden mejorar significativamente su resiliencia ante posibles amenazas, promoviendo al mismo tiempo la eficiencia y efectividad en la gestión de riesgos cibernéticos [24].

Por otra parte, la actualización NIST 800-53 Rev. 4 a NIST 800-53 Rev. 5 presenta mejoras significativas en los controles de privacidad y seguridad de los sistemas de información. La versión 5 integra la seguridad y la privacidad de manera más consistente, estableciendo controles específicos para proteger los datos personales y reducir los riesgos

asociados. Estos controles incluyen métodos para disminuir la recopilación y el uso de datos personales, garantizar la transparencia y garantizar que las personas participen en la gestión de sus datos [25].

1.1.19 OWASP Top 10

La Open Web Application Security Project (OWASP) desempeña un papel fundamental en la mejora de la seguridad en aplicaciones web al publicar la lista conocida como OWASP Top 10. Este recurso identifica las diez vulnerabilidades más críticas que pueden afectar a aplicaciones web, proporcionando a los profesionales de la ciberseguridad una guía estratégica para concentrar sus esfuerzos en las áreas más vulnerables y críticas. La lista aborda una amplia gama de amenazas, desde la inyección de código hasta la exposición de datos sensibles, brindando así una visión integral de las debilidades más prevalentes en el panorama de seguridad web. La adopción de las recomendaciones de OWASP Top 10 no solo fortalece las defensas de las aplicaciones web, sino que también contribuye a elevar el estándar general de seguridad en el desarrollo y mantenimiento de estas aplicaciones [26].

1.1.20 SANS Critical Security Controls

La lista de controles de seguridad críticos de SANS es una guía importante que incluye veinte controles prioritarios, brindando a las organizaciones un marco detallado para mejorar significativamente su postura de seguridad. Esta compilación, creada por el Instituto SANS, funciona como un recurso completo que aborda una variedad de aspectos importantes de la ciberseguridad. Esta lista proporciona un enfoque estratégico para reducir riesgos y fortalecer las defensas al concentrarse en controles esenciales, como la gestión de inventario de hardware y software y la monitorización continua de la seguridad. La implementación de estos controles no solo proporciona una base sólida para la seguridad, sino que también ayuda a las organizaciones a adaptarse proactivamente a las amenazas emergentes en el mundo digital en constante cambio [27].

1.1.21 COSO

Es ampliamente utilizado para evaluar y mejorar los sistemas de control interno de las organizaciones, y es conocido por su marco de control interno, "COSO Internal Control - Integrated Framework". Aunque no está diseñado específicamente para la ciberseguridad, se puede modificar para incluir temas de seguridad de datos. Por ejemplo, el marco COSO enumera elementos importantes de control interno, como el ambiente de control, la evaluación de riesgos y las actividades de control. Estos elementos también son pertinentes a la gestión de la ciberseguridad. El marco COSO se puede utilizar para evaluar la ciberseguridad de una organización al incorporar medidas de seguridad de la información en estos componentes [20].

1.1.22 COBIT

COBIT es un marco de gestión de tecnología de la información que se centra en proporcionar guías para la gobernanza y el control de los procesos de TI dentro de las organizaciones. Este marco incluye objetivos de control específicos relacionados con la seguridad de la información y la ciberseguridad. COBIT 2019, en particular, ha integrado un enfoque de gestión de ciberseguridad que aborda aspectos fundamentales como la identificación y protección de activos de información, la detección y respuesta a riesgos de seguridad, y la recuperación tras un ataque [28].

1.1.23 Normativa Importante y su evolucion

La evolución de las amenazas cibernéticas recuerda constantemente la importancia de estar al día con los estándares y marcos más recientes de seguridad de la información. Se han producido cambios significativos en el último año que reflejan la necesidad de adaptarse a un entorno digital en constante evolución. Entre estos cambios se encuentra la entrada en vigor de la norma ISO 27001:2022, que ha simplificado su estructura al reducir el número de controles y ha agregado once nuevos controles específicos para la ciberseguridad. Esta actualización es un avance en la gestión proactiva de riesgos que permite a las organizaciones abordar de manera más efectiva las amenazas emergentes [22]. A continuación, se presenta un resumen de los aspectos más relevantes de esta transición:

- **Reducción y reestructuración de controles**:

Se simplifica la cantidad de controles de 114 a 93, agrupados en 4 dominios en lugar de los 14 dominios previos. Esta consolidación busca facilitar la comprensión e implementación del estándar.

Los 4 dominios que estructuran los controles en la versión 2022 son:

1. Controles Organizacionales (37 controles)
2. Controles de Personas (8 controles)
3. Controles Físicos (14 controles)
4. Controles Tecnológicos (34 controles)

Nuevos controles para un panorama de amenazas en constante evolución: Se incorporan 11 nuevos controles para abordar las ciberamenazas actuales y las prácticas de seguridad emergentes. Estos controles abarcan aspectos como:

- Inteligencia de amenazas
- Seguridad de la información en la nube
- Gestión de la configuración
- Eliminación de información

- Enmascaramiento de datos
- Prevención de fuga de datos
- Monitoreo de actividades
- Seguridad de la información en el uso de servicios en la nube
- Preparación de las TIC para la continuidad del negocio
- Monitoreo de la seguridad física.

- **Normatividad actualizada**

Teniendo en cuenta lo reseñado anteriormente, a continuación se bosqueja un análisis de las normas recientes, con énfasis en el contexto de la organización: la norma 2022 resalta la comprensión del contexto de la organización y su entorno para una implementación efectiva del SGSI. Esto implica identificar las necesidades y riesgos específicos de la organización para adaptar los controles de manera adecuada. Mayor enfoque en el liderazgo y la responsabilidad: Se refuerza la importancia del liderazgo y la responsabilidad de la alta dirección en la gestión de la seguridad de la información. Esto involucra un compromiso activo para establecer, implementar y mantener el SGSI [29]. Adopción de un enfoque basado en riesgos: Se reitera la importancia de un enfoque basado en riesgos para la gestión de la seguridad de la información. Esto implica identificar, evaluar y tratar los riesgos de manera sistemática y proporcional. Actualización con las últimas prácticas y tecnologías: La norma se actualiza para reflejar las últimas prácticas, tecnologías y amenazas en el ámbito de la seguridad de la información. Implementación y auditoría: Las organizaciones certificadas bajo ISO 27001:2013 tienen un plazo de 3 años para realizar la transición a la nueva versión 2022 [30]. En resumen, la transición a ISO 27001:2022 implica una adaptación a un enfoque más simplificado, robusto y actualizado de la gestión de seguridad de la información, alineado con las amenazas y desafíos actuales.

Además, la ISO 27005:2022 se ha ampliado para reflejar la convergencia entre la seguridad de la información, la seguridad cibernética y la protección de la privacidad. Esta actualización ofrece un enfoque más completo y integral para la gestión de riesgos de seguridad de la información al alinearse con otras normas clave, como ISO/IEC 27001:2022 e ISO 31000:2018, y al incluir nuevos conceptos como "escenarios de riesgo". Este cambio refleja la necesidad de una evaluación más profunda y compleja de los riesgos en un entorno digital cada vez más complejo [31].

Sin embargo, la actualización del NIST Cybersecurity Framework a la versión 2.0 agregó una nueva función de gobierno y reorganizó las subcategorías entre las funciones ya existentes. Esta evolución muestra una respuesta activa a los desafíos cambiantes del entorno de ciberseguridad, reconociendo la importancia de una gobernanza efectiva en la gestión de riesgos. Esta actualización brinda a las empresas una estructura más sólida y adaptable para mejorar su enfoque en la seguridad cibernética [24].

Las normas ISO 27005 e ISO 19011, junto con el enfoque GRC (Gobierno, Riesgo, Cumplimiento), juegan un papel importante en la gestión de riesgos y la auditoría de sistemas

de gestión, proporcionando directrices específicas y un marco integral para fortalecer la seguridad de la información y garantizar el cumplimiento normativo [32].

Por su parte, la norma ISO 27005:2022 se enfoca en la gestión de riesgos de seguridad de la información y proporciona pautas para garantizar que la confidencialidad, la integridad y la disponibilidad de la información en una organización estén protegidas. Independientemente de su tamaño o sector, su alcance se extiende a todas las organizaciones. Para mejorar el enfoque de gestión de riesgos, la norma incorpora el concepto de "escenarios de riesgo" y se alinea con otras normas importantes como ISO/IEC 27001:2022 e ISO 31000: 2018 [33].

Sin embargo, la norma ISO 19011:2018 establece pautas para la auditoría de sistemas de gestión, que incluyen sistemas de gestión de la seguridad de la información (SGSI) certificados bajo la norma ISO 27001 [34]. Esta regla es válida para las empresas que contratan auditores externos o realizan auditorías internas para evaluar la conformidad de sus sistemas de gestión. La definición de principios, requisitos e instrucciones para la planificación, realización e informe de auditorías, así como un enfoque adaptable que se adapta a diferentes tipos de sistemas de gestión y necesidades organizativas específicas, son sus características principales.

El enfoque GRC mejora el control interno, la toma de decisiones y el cumplimiento de las regulaciones aplicables al integrar los principios de gobierno, riesgo y cumplimiento en la gestión de una organización. Este método se aplica a todos los aspectos de la gestión de una organización, desde la estrategia hasta las operaciones diarias. El establecimiento de una estructura de gobierno clara, la implementación de un proceso de gestión de riesgos y la garantía de cumplimiento con las leyes y regulaciones son sus características principales [24].

Por último, pero no menos importante, la Revisión 5 de la publicación NIST 800-53 agregó nuevos controles para abordar temas importantes de seguridad y privacidad de datos personales. Este cambio refleja la preocupación creciente por la privacidad en un mundo digital cada vez más interconectado y basado en datos. Las organizaciones pueden reducir de manera más efectiva los riesgos asociados con el manejo y procesamiento de datos personales sensibles al incluir estos controles en su enfoque de seguridad de la información [25].

Además de las normas internacionales mencionadas anteriormente, existen numerosas normas internacionales relacionadas con la auditoría de seguridad de los sistemas SCADA. Estas normas brindan directrices específicas sobre cómo evaluar e implementar los controles de seguridad de estos sistemas [26].

La serie ISA/IEC 62443 proporciona un marco completo para la seguridad de los sistemas de control industrial (ICS). Las pautas específicas para la auditoría de seguridad de SCADA se encuentran en la Parte 3-3 de esta serie, titulada "Ciberseguridad para sistemas y componentes industriales - Parte 3-3: Especificaciones de seguridad para sistemas de control y supervisión (SCADA) y sistemas de adquisición de datos (DAS)" [35].

Una guía para realizar evaluaciones de riesgo de seguridad de la información en sistemas de control industrial es la publicación NIST SP 800-82 del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. La norma internacional IEC 62351 especifica las normas de seguridad para los sistemas de control industrial y los componentes

de seguridad. Esta norma trata temas como la gestión de riesgos, la seguridad del producto, la seguridad de la red y la seguridad operativa, todos ellos relacionados con la auditoría de seguridad de SCADA. Además, la norma IEEE 1686-2007 proporciona instrucciones sobre cómo aplicar medidas de seguridad física y lógica a los sistemas de control industrial. Esta guía proporciona pautas específicas para el control de acceso físico, la seguridad de la red, la seguridad del software y la seguridad de los datos en entornos SCADA [25].

Teniendo en cuenta lo expuesto en los párrafos anteriores y con el fin de profundizar en la Norma ISO, es importante destacar que la seguridad de la información es un aspecto crucial para las organizaciones en la era digital, donde las amenazas cibernéticas y las vulnerabilidades tecnológicas evolucionan constantemente. Para ayudar a las organizaciones a proteger su información y gestionar los riesgos asociados, la Organización Internacional de Normalización (ISO) ha desarrollado una serie de estándares. Entre ellos tal como se ha mencionado, la ISO 27002 y la ISO 27005 son fundamentales. La ISO 27002 proporciona directrices para implementar controles de seguridad de la información, mientras que la ISO 27005 ofrece un marco para la gestión de riesgos de seguridad de la información. Ambas normas han sido actualizadas recientemente, en 2022, para abordar mejor los desafíos actuales y emergentes en la seguridad de la información. Esta revisión se enfoca en analizar los cambios significativos introducidos en las versiones más recientes de estos estándares, destacando cómo se alinean con las mejores prácticas modernas y las necesidades contemporáneas de seguridad [36].

La ISO 27002:2013, como un estándar que proporciona directrices para las prácticas de gestión de la seguridad de la información, se estructura en torno a 14 dominios de control que abordan aspectos cruciales como políticas de seguridad, organización de la seguridad, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad en las operaciones, comunicaciones, desarrollo y mantenimiento de sistemas, relaciones con proveedores, gestión de riesgos, continuidad del negocio y cumplimiento [37].

La ISO 27002:2022 introduce cambios significativos para alinearse mejor con las necesidades actuales de seguridad y las amenazas emergentes. Los controles se han reducido de 114 a 93 y se han reorganizado en cuatro temas principales: Organización, Personas, Tecnologías y Proceso. Además, se han añadido 11 nuevos controles que abordan aspectos como inteligencia sobre amenazas, seguridad en la ingeniería, configuración segura, gestión de identidad, autenticación y credenciales. Varios controles existentes han sido modernizados para reflejar mejor las prácticas actuales y las tecnologías emergentes. Los controles ahora tienen atributos específicos que ayudan a las organizaciones a clasificarlos y gestionarlos más fácilmente, como tipo de control, propiedad de seguridad, ciberseguridad y capacidades operacionales [38].

La ISO 27002:2022 está alineada con la ISO 27001:2022, lo que requiere que las organizaciones que implementan un Sistema de Gestión de Seguridad de la Información (SGSI) ajusten sus políticas y procedimientos para alinearse con los nuevos controles. Esta alineación facilita la implementación de un SGSI coherente y actualizado que responde a las necesidades de seguridad contemporáneas [39].

Por otro lado, la ISO 27005:2018 proporciona directrices para la gestión de riesgos de seguridad de la información, ayudando a las organizaciones a identificar, evaluar y tratar los

riesgos en alineación con ISO 27001. La ISO 27005:2022 introduce varios cambios y mejoras importantes para hacer frente a las nuevas amenazas y mejorar la gestión del riesgo. Uno de los cambios más significativos es el mayor enfoque en el contexto organizacional y en las partes interesadas al evaluar los riesgos [40].

Además, la actualización de términos y definiciones para alinearse con la terminología actual de gestión de riesgos y seguridad de la información, junto con una mejor integración con ISO 31000, facilita una integración más fluida con los sistemas de gestión de riesgos organizacionales generales. La ISO 27005:2022 también enfatiza el ciclo de vida completo del riesgo, incluyendo identificación, evaluación, tratamiento, monitoreo y revisión, y proporciona más orientación práctica y ejemplos para ayudar a las organizaciones a implementar de manera efectiva la gestión de riesgos de seguridad de la información. Se destaca la necesidad de una evaluación y monitoreo continuo de los riesgos, considerando el entorno cambiante de amenazas [40].

En conclusión, las actualizaciones de la ISO 27002:2022 y la ISO 27005:2022 reflejan un esfuerzo por modernizar y hacer más relevantes los estándares de gestión de la seguridad de la información y de gestión de riesgos [40]. Estas actualizaciones están diseñadas para ayudar a las organizaciones a enfrentar las amenazas actuales y emergentes de manera más efectiva, asegurando que los controles y procesos de gestión de riesgos estén alineados con las mejores prácticas y tecnologías actuales.

- **NIST CSF 1.1**

El Framework para la Mejora de la Seguridad Cibernética de las Infraestructuras Críticas (NIST CSF) versión 1.1, publicado por el Instituto Nacional de Estándares y Tecnología (NIST), está diseñado para ayudar a las organizaciones a gestionar y reducir los riesgos de ciberseguridad. La versión 1.1 del NIST CSF se estructura en torno a cinco funciones principales: Identificar, Proteger, Detectar, Responder y Recuperar. Cada función está dividida en categorías y subcategorías específicas que detallan los procesos y actividades necesarios para alcanzar los objetivos de ciberseguridad [41].

1. Identificar: Enfoque en la comprensión del entorno organizacional para gestionar mejor los riesgos.
2. Proteger: Implementación de salvaguardas para asegurar los servicios críticos.
3. Detectar: Desarrollar y realizar actividades de monitoreo para identificar la ocurrencia de un evento cibernético.
4. Responder: Realizar actividades de respuesta ante un riesgo de ciberseguridad.
5. Recuperar: Implementar planes de recuperación para restaurar las capacidades afectadas por riesgos de ciberseguridad.

- **NIST CSF 2.0**

La versión 2.0 del NIST CSF introduce una sexta función, Gobierno, que aborda la planificación, estrategias y gobernanza de la gestión de riesgos de ciberseguridad dentro de una organización. Con esta nueva función, el marco ahora comprende seis funciones clave: Identificar, Proteger, Detectar, Responder, Recuperar y Gobierno. La función de Gobierno incluye 31 subcategorías adicionales y redistribuye algunas de las subcategorías existentes para adaptarse a esta nueva estructura [42].

1. Identificar: Continúa enfocándose en la comprensión del entorno organizacional para gestionar mejor los riesgos, pero ahora con una integración más clara con las estrategias de gobernanza [42].
2. Proteger: Sigue abarcando las salvaguardas para asegurar los servicios críticos, incorporando nuevas subcategorías para reflejar las mejores prácticas actuales.
3. Detectar: Mantiene su enfoque en el monitoreo de eventos cibernéticos, con actualizaciones para mejorar la detección temprana de amenazas.
4. Responder: Actualizaciones en las actividades de respuesta ante riesgos, alineándose con las nuevas subcategorías y estrategias de gobernanza.
5. Recuperar: Enfoque mejorado en los planes de recuperación, integrando lecciones aprendidas y nuevas prácticas de recuperación.
6. Gobierno: Nueva función que cubre la estructura de gobernanza de la ciberseguridad, incluyendo 31 subcategorías que abordan la planificación, estrategias, roles, responsabilidades y procesos de gestión de riesgos. Esta función asegura que la ciberseguridad se integre en todos los niveles de la organización y se alinee con los objetivos empresariales.

- **Redistribución de Subcategorías**

Para acomodar la nueva función de Gobierno, algunas subcategorías de las funciones anteriores fueron redistribuidas y se crearon nuevas subcategorías. Esta redistribución asegura que todas las áreas clave de ciberseguridad y gobernanza se aborden de manera integral y coherente.

1. Subcategorías Redistribuidas: Algunas subcategorías de "Identificar" y "Proteger" ahora se encuentran bajo "Gobierno" para reflejar mejor su papel en la estrategia y gobernanza organizacional.
2. Nuevas Subcategorías: Se han añadido nuevas subcategorías dentro de "Gobierno" y las otras funciones para abordar las necesidades emergentes y mejores prácticas en ciberseguridad.

En síntesis, las actualizaciones del NIST CSF 2.0 reflejan un esfuerzo por mejorar la relevancia y efectividad del marco en la gestión de riesgos de ciberseguridad. La adición de la función de Gobierno y la redistribución de subcategorías proporcionan una estructura más robusta y completa para que las organizaciones integren la ciberseguridad en su estrategia y gobernanza global. Estos cambios están diseñados para ayudar a las organizaciones a enfrentar de manera más efectiva las amenazas cibernéticas actuales y emergentes, asegurando que las prácticas de ciberseguridad estén alineadas con los objetivos y procesos organizacionales [31].

- **NIST 800-53 Rev. 4**

La NIST 800-53 Rev. 4, publicada en 2013, se centraba en proporcionar controles de seguridad para sistemas de información federales. Esta versión incluía una estructura organizada en 18 familias de controles, tales como Control de Acceso, Auditoría y Rendición de Cuentas, y Gestión de Configuración. Los controles estaban diseñados para mitigar una amplia gama de riesgos de seguridad y asegurar la protección adecuada de los datos [43].

- **NIST 800-53 Rev. 5**

La NIST 800-53 Rev. 5, publicada en 2020, introduce una serie de actualizaciones y mejoras significativas para abordar las necesidades actuales de seguridad y privacidad. Una

de las incorporaciones más destacadas es el énfasis reforzado en la privacidad de los datos personales. La revisión 5 no solo amplía la cantidad y el alcance de los controles de seguridad, sino que también introduce controles específicos para la privacidad, integrándolos en las familias existentes y creando nuevas subcategorías donde sea necesario [43].

1. Incorporación de Nuevos Controles de Seguridad y Privacidad:
    - La Rev. 5 introduce nuevos controles específicos que abordan la protección de la privacidad de los datos personales, reflejando una mayor preocupación por el manejo y la protección de la información personal.
    - Se añaden controles para gestionar la privacidad desde el diseño (Privacy by Design), garantizando que las consideraciones de privacidad se integren desde el inicio en los procesos y sistemas.
2. Alineación con Otros Marcos y Normas:
    - La nueva versión alinea mejor los controles de seguridad y privacidad con otros marcos y estándares internacionales, como el RGPD (Reglamento General de Protección de Datos) y el NIST Privacy Framework, facilitando la interoperabilidad y el cumplimiento multijurisdiccional.
    - Esta alineación ayuda a las organizaciones a implementar controles consistentes y armonizados que cumplen con múltiples requisitos regulatorios y normativos.
3. Mayor Énfasis en la Gestión de la Cadena de Suministro:
    - La Rev. 5 incorpora controles mejorados para gestionar los riesgos en la cadena de suministro, asegurando que las organizaciones consideren la seguridad y la privacidad a lo largo de toda la cadena de suministro y no solo dentro de sus propios límites.
    - Estos controles incluyen la evaluación de proveedores y la gestión de riesgos asociados con terceros y servicios en la nube.
4. Actualización y Expansión de Controles Existentes:
    - Se revisan y expanden varios controles existentes para abordar las amenazas emergentes y las mejores prácticas actuales. Esto incluye la incorporación de tecnologías emergentes como la inteligencia artificial y el Internet de las cosas (IoT).
    - Además, se incluyen más directrices sobre cómo implementar y mantener estos controles de manera efectiva, proporcionando ejemplos prácticos y casos de uso.
5. Enfoque en la Resiliencia y Recuperación:

- Se fortalecen los controles relacionados con la resiliencia operativa y la recuperación ante riesgos, asegurando que las organizaciones puedan mantener operaciones críticas y recuperarse rápidamente de interrupciones.
- Estos controles también incluyen estrategias para la continuidad del negocio y la recuperación de desastres, integrando aspectos de seguridad y privacidad en estos procesos [44].

En conclusión, la transición de la NIST 800-53 Rev. 4 a la Rev. 5 representa una evolución significativa en la forma en que se abordan la seguridad y la privacidad de la información. Con la incorporación de nuevos controles específicos de privacidad, una mejor alineación con otros marcos internacionales, y un enfoque reforzado en la gestión de la cadena de suministro y la resiliencia operativa, la Rev. 5 proporciona a las organizaciones una guía más completa y actualizada para enfrentar los desafíos contemporáneos de ciberseguridad y protección de datos personales. Esta actualización asegura que las prácticas de seguridad y privacidad estén bien integradas y sean efectivas en un entorno digital cada vez más complejo y regulado.

1.1.24 Análisis del Concepto de Infraestructuras Críticas en Colombia

Adicional a lo expuesto anteriormente, es importante resaltar que en la actualidad, las infraestructuras críticas (IC) se han convertido en elementos esenciales para el funcionamiento de las sociedades modernas. Estas infraestructuras abarcan una amplia gama de sectores, incluyendo energía, transporte, comunicaciones, salud, agua y saneamiento, y servicios financieros. Su correcto funcionamiento es vital para garantizar la seguridad nacional, la salud pública, el bienestar económico y la calidad de vida de los ciudadanos [45].

En lo que respecta al caso específico de Colombia el concepto de infraestructuras críticas se define en la Ley 800 de 2014 como "aquellas instalaciones, redes, servicios y activos físicos y de la información esenciales para el funcionamiento de las actividades económicas, sociales y ambientales del país, cuya afectación o destrucción tendría un impacto significativo en la salud, la seguridad, el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado en todos sus niveles de administración pública" [46].

- **Aplicación en Sectores Claves en Colombia con infraestructuras críticas.**

La presencia de infraestructuras críticas se extiende a diversos sectores, cada uno con características y desafíos únicos en materia de seguridad y ciberseguridad. A continuación, se profundiza en algunos de los sectores claves:

- Sector de energía: Incluye la generación, transmisión y distribución de energía eléctrica, así como la producción y transporte de combustibles. Las infraestructuras críticas en este sector son altamente vulnerables a ataques cibernéticos que podrían provocar apagones masivos, interrupciones en la cadena de suministro de energía y graves consecuencias para la economía y la sociedad.

- Sector de transporte: Comprende la red vial, ferroviaria, aérea y marítima, así como los sistemas de control de tráfico y los servicios de transporte público. Las infraestructuras críticas en este sector son susceptibles a ataques que podrían ocasionar accidentes, disrupciones en la movilidad, daños económicos y perjuicios a la población.

- Sector de comunicaciones: Incluye la infraestructura de telecomunicaciones, como redes móviles, fijas y satelitales, así como los centros de datos y los servicios de internet. Las infraestructuras críticas en este sector son esenciales para la comunicación, el comercio electrónico y la prestación de servicios públicos. Su afectación podría generar caos social, interrupciones en la actividad económica y fallas en la prestación de servicios esenciales.

- Sector de salud: Abarca los hospitales, clínicas, laboratorios, bancos de sangre y sistemas de atención médica de emergencia. Las infraestructuras críticas en este sector son fundamentales para la salud pública y la protección de la vida. Su afectación podría ocasionar la suspensión de servicios médicos críticos, la pérdida de datos de pacientes y poner en riesgo la vida de las personas [46].

- **Conexión de los SCADA en los Sistemas de Control Industrial.**

Los sistemas de control y adquisición de datos (SCADA) desempeñan un papel crucial en la operación de las infraestructuras críticas, permitiendo el monitoreo, control y gestión de los procesos industriales en tiempo real. La conexión de los SCADA a las redes de comunicación y a internet los expone a una amplia gama de amenazas cibernéticas que podrían comprometer la seguridad y la integridad de las infraestructuras críticas [47].

- **Importancia de la ciberseguridad en las infraestructuras críticas.**

La ciberseguridad es un aspecto fundamental en la protección de las infraestructuras críticas. Los ataques cibernéticos a estas infraestructuras podrían tener consecuencias devastadoras, incluyendo:

- Interrupciones en la prestación de servicios esenciales: Apagones, cortes de agua, interrupciones en el transporte y la comunicación, y fallas en la atención médica.
- Daños económicos: Pérdidas financieras directas e indirectas, impacto en la productividad y el comercio, y afectación a la imagen y reputación de las organizaciones.
- Riesgos para la seguridad pública: Accidentes en el sector transporte, sabotaje a instalaciones energéticas, y riesgos para la salud pública en el sector sanitario.
- Pérdida de confianza en las instituciones: Erosión de la confianza pública en la capacidad del Estado para proteger sus infraestructuras críticas [48].

- **Impactos por la materialización de un incidente de seguridad y/o ciberseguridad.**

La materialización de un riesgo de seguridad o ciberseguridad en una infraestructura crítica puede generar una serie de impactos negativos, que varían en función del sector afectado, la gravedad del riesgo y las medidas de respuesta implementadas. Algunos de los impactos potenciales incluyen:

- Daños físicos: Destrucción o inhabilitación de equipos y sistemas, interrupciones en la operación de las infraestructuras, y riesgos para la seguridad de las personas y el medio ambiente.
- Daños Económicos: Los costos asociados con la interrupción de servicios y la restauración de infraestructuras dañadas podrían ser enormes, afectando negativamente la economía del país y las empresas afectadas.
- Impacto en la Salud Pública: Un riesgo que afecte las infraestructuras de salud o saneamiento podría causar brotes de enfermedades, contaminación ambiental y otros riesgos para la salud pública.
- Inestabilidad Social: La interrupción de servicios básicos como el suministro de energía o el transporte público podría causar inestabilidad social, protestas y disturbios civiles [49].

Por último, se destaca que la seguridad de las infraestructuras críticas en Colombia es de vital importancia para la estabilidad económica, social y política del país. La conexión de estas infraestructuras con los sistemas de control industrial introduce nuevos desafíos en términos de seguridad cibernética, que deben ser abordados con urgencia. Es fundamental que el gobierno, las empresas y la sociedad en su conjunto reconozcan la importancia de proteger estas infraestructuras y tomen medidas proactivas para mitigar los riesgos y fortalecer la resiliencia ante posibles amenazas de seguridad y ciberseguridad.

1.1.25 Tipos de Gestión de Riesgo

Para comprender a fondo los conceptos que se utilizarán en la propuesta de investigación, es fundamental definir claramente los términos "riesgo" y "control". En la gestión de riesgos, "riesgo" se refiere a la posibilidad de que ocurra un evento adverso que pueda afectar negativamente los objetivos de una organización. El concepto se divide en tres categorías: el riesgo inherente, que es el nivel de riesgo antes de implementar cualquier control; el riesgo con control, que es el riesgo que persiste después de implementar controles preventivos; y el riesgo residual, que es el riesgo que persiste después de implementar medidas de mitigación. Sin embargo, los "controles" son acciones o medidas que una organización toma para reducir la probabilidad o el impacto de las amenazas. Estos controles pueden ser preventivos, que se aplican antes de que ocurra un evento adverso para evitar que se materialice, o correctivos, que se aplican después de que ocurra el evento para reducir su impacto y evitar que ocurra de nuevo [8].

Hacia una gestión de riesgos efectiva, es necesario comprender estas definiciones. Las organizaciones pueden crear planes para reducir los riesgos identificando y evaluando los riesgos de manera precisa. Por ejemplo, se puede determinar la eficacia de los controles existentes y la necesidad de medidas adicionales al distinguir entre el riesgo inherente y el riesgo residual. Además, al entender la diferencia entre controles preventivos y correctivos, las organizaciones pueden priorizar sus acciones de seguridad concentrándose en la prevención de eventos adversos y en la capacidad de responder adecuadamente en caso de que ocurran. Esta comprensión ayuda a todas las partes interesadas a comunicar los riesgos y las estrategias de mitigación de manera clara y concisa, lo que es esencial para una gestión de riesgos efectiva [9].

Al mismo tiempo, en el contexto de la seguridad de los sistemas de control y adquisición de datos industriales (SCADA), los conceptos de riesgo inherente, riesgo con control y riesgo residual son fundamentales para comprender el nivel de protección general y tomar las medidas adecuadas para mitigar las amenazas [21].

Riesgo Inherente o Absoluto: El riesgo inherente, también conocido como riesgo absoluto, representa el nivel de riesgo que existe en un sistema SCADA sin la aplicación de ningún control de seguridad. Este riesgo se basa en las características inherentes del sistema, sus vulnerabilidades y las amenazas potenciales a las que está expuesto. El riesgo inherente es un indicador del nivel de exposición inicial del sistema antes de implementar medidas de protección [21].

Riesgo con Control: El riesgo con control, también conocido como riesgo residual modificado, refleja el nivel de riesgo que queda después de implementar controles de seguridad en el sistema SCADA. Estos controles pueden incluir medidas preventivas, como firewalls, autenticación y cifrado, así como medidas correctivas, como planes de respuesta a riesgos y recuperación de desastres. El riesgo con control indica el nivel de protección que se ha logrado mediante la implementación de medidas de seguridad [50].

Riesgo Residual: El riesgo residual representa el nivel de riesgo que persiste incluso después de aplicar controles de seguridad en el sistema SCADA. Este riesgo residual se debe a que ningún control de seguridad es perfecto y siempre existe la posibilidad de que las amenazas puedan eludir las medidas implementadas. El riesgo residual es un indicador del nivel de riesgo que aún permanece después de tomar las medidas de protección adecuadas.

Controles de Seguridad: Los controles de seguridad son medidas y procedimientos implementados para mitigar los riesgos y proteger los sistemas SCADA de amenazas potenciales. Estos controles se clasifican en dos categorías principales:

1. Controles Preventivos: Los controles preventivos tienen como objetivo evitar que ocurran riesgos de seguridad. Estos controles se enfocan en la identificación y eliminación de vulnerabilidades en el sistema, la implementación de medidas de protección como firewalls y autenticación, y la capacitación del personal en prácticas de seguridad.
2. Controles Correctivos: Los controles correctivos tienen como objetivo minimizar el impacto y la recuperación en caso de que ocurra un riesgo de seguridad. Estos controles incluyen planes de respuesta a riesgos, procedimientos de recuperación de desastres, y mecanismos para el análisis forense y la evidencia digital [51].

La comprensión de los conceptos de riesgo inherente, riesgo con control y riesgo residual, junto con la implementación efectiva de controles preventivos y correctivos, es esencial para gestionar de manera adecuada los riesgos de seguridad en los sistemas SCADA. Una evaluación continua de los riesgos y la adaptación de las medidas de protección son fundamentales para mantener una postura de seguridad robusta y proteger los activos críticos de las organizaciones [51].

1.1.26 Los roles y acciones que realizan las 3 líneas de defensa

Desde el aspecto de los roles y acciones es importante resaltar que tres líneas principales dentro de una organización son la gestión de activos, riesgos y controles. Los procesos directamente responsables de la gestión de estos aspectos, como la realización de autoevaluaciones, el cumplimiento de políticas, la gestión de riesgos y la implementación de controles, se denominan roles de primera línea. Los roles de segunda línea incluyen la verificación de la identificación de riesgos, la evaluación de los controles existentes, la garantía del cumplimiento de las políticas y la propuesta de inversiones, así como el apoyo a su ejecución. Por otro lado, los roles de tercera línea son responsables de verificar independientemente el cumplimiento del marco de gobierno establecido en la organización, minimizar el riesgo y asegurar el logro de los objetivos [52].

1.2 Estado del arte

En el presente las infraestructuras criticas (IC) más conocidas como sistemas de automatización industrial que tienen como funcionalidad proveer servicios esenciales a nivel mundial como son el suministro de energía, agua, gas, petróleo, transporte y demás dispositivos que llevan instrucciones lógicas para el buen desarrollo de su función además de la captación de información para su estudio monitoreo para la generación de reportes y la mejor toma de decisiones. Teniendo en cuenta la realidad del caso que a continuación se describe se establece que un sistema SCADA es de una funcionalidad permanente para su buen aprovechamiento con referencia a lo dicho anteriormente se entendió que estos sistemas son propensos a diversos ataques por su función tan importante en la sociedad y que cada día se van incrementando. Para entender un poco más a fondo dicho proceso de este objetivo primero se desarrolla un mapa de riesgos teniendo en cuenta la norma ISO 27005 donde se aplica los procesos de dicha norma que a continuación se describirán.

En los sistemas industriales SCADA al conocer la situación de los sensores que lo componen permite obtener los datos sobre su proceder de esta manera se logra concluir efectos y adecuar distintos métodos que cooperen a estrechar el riesgo cibernético. en una búsqueda solicitada, se expone un sistema de pronóstico de probables ciberataques en un sistema SCADA. Dicha predicción se ejecuta mediante un filtro Kalman que produce hechos de ciberseguridad reflejados a través del sistema de detección de intrusos (aplicado en un sistema de simulación de SCADA) y origina un alcance futuro de probabilidades que se consoliden en un agravio empresarial, teniendo en cuenta estas notificaciones los administradores de sistemas lograrán escoger alguna elección acerca de cómo proceder frente a próximos ataques informáticos [51].

Todos los datos de una organización son considerados en la actualidad como uno de los elementos más valioso concerniente a su capacidad competitiva, por lo cual, procesar los datos en los encausamientos industriales hace que el uso de sistemas SCADA sean necesarios para las empresas que usan este modelo para optimizar tanto la eficiencia y eficacia en los procesos así como adicionalmente para asistir a la seguridad industrial, señalando que con la competencia en crecimiento igualmente se manifiesta de forma coherente riesgos que colocan en amenaza el proceder de la empresa dada esta circunstancia se expone un método

con el fin de dirigir el procedimiento de inspección, con el propósito de aplacar el riesgo en el área operacional de la organización [52].

Hoy en día, la ciberseguridad se ha vuelto un estándar esencial para la mayoría de las organizaciones, ya que engloba diversas técnicas seguras en el campo de la tecnología de la información. Los sistemas críticos SCADA, ahora integrados en los sistemas de Tecnologías de la Información (TI), están expuestos a ciberataques que anteriormente se dirigían principalmente a las TI tradicionales. El aumento de riesgos en los sistemas SCADA ha generado brechas de seguridad, requiriendo que las empresas supervisen de cerca procesos críticos, sistemas, máquinas y líneas de producción. En entornos más complejos, como el suministro de electricidad y la refrigeración de sistemas, es crucial mantener un conocimiento constante de los procesos. Aunque los sistemas SCADA pueden ser desconocidos para gran parte de la sociedad, desempeñan un papel fundamental en la toma de decisiones ante averías o mal funcionamiento, respaldando una gestión efectiva y en tiempo real de diversas actividades empresariales. La seguridad ocupa un lugar central, ya que una falla en estos procesos podría resultar en pérdidas económicas significativas, daños ambientales graves e incluso riesgos para la vida humana [53].

Los riesgos generados por los ciberataques está aumentando en los sistemas de control industrial (ICS), cuya función se enmarca principalmente en las infraestructuras críticas (CI) y como resultado, las organizaciones deben establecer un mecanismos que permita la mejora en la respuesta ante la ocurrencia de eventos de seguridad, lo que implica la necesidad se sincronizar los diferentes departamentos internos y el proceso de auditoría, sin embargo, muchas organizaciones ven esta sincronización como innecesaria o poco práctica, dado los intereses particulares de los administradores de los SCADAS y los de las redes de computadores tradicionales [54].

Las organizaciones dependen de la gestión constante de la infraestructura crítica, pero las amenazas de ciberseguridad se aprovechan de la complejidad del sistema y su conexión. Esto implica riesgos significativos para la seguridad nacional, la economía, la salud y la seguridad pública, así como para la reputación y las finanzas. Estos riesgos cibernéticos afectan el rendimiento de una organización, aumentando costos e impactando los ingresos. La ciberseguridad se vuelve crucial para la administración total de riesgos de una empresa, especialmente en los 16 sectores críticos de infraestructura que son esenciales para cualquier nación. Estos sectores incluyen sistemas y redes, tecnología de la información, comunicaciones, instalaciones comerciales, fabricación crítica, represas, defensa industrial, servicios de emergencia, energía, servicios financieros, agroalimentario, sistemas de agua y aguas residuales, entre otros [55].

Es relevante explicar que hay diversos ejemplos de regulación para estos sistemas de control, centradas particularmente para la protección de estos sistemas sus datos y comunicaciones, en el que se recolectan distintas referencias y sugerencias, por lo tanto, hay esquemas enfocados en sectores particulares, tal como el energético. Una recolección total de esta reglamentación es la que ofrece INCIBE en su página oficial, existen análisis en la cual emplean esta normalización. En el caso del estudio para los sistemas SCADA realizado por Czechowski, Wicher y Wiecha y el proceso comunicacional, se ha aplicado la normativa IEC 61850 [50], en esta se define una serie de procedimientos de cómo identificar las diferentes vulnerabilidades para un escenario, entre las vulnerabilidades figura “valores de

usuario y contraseña por defecto", lo que implica un problema grave a solucionar, pero como lo indican las normas, se da el "que" pero no el "cómo" aplicar una respuesta oportuna.

Por otro lado, [52]. presenta una propuesta de "metodología para la auditoría de ciberseguridad aplicada a un sistema SCADA", y define varios parámetros a seguir desde la gestión de riesgos, considerando pasos como el levantamiento de información, planificación de la estrategia, obtención de vulnerabilidades, priorización de los riesgos y presentación de resultados, sin embargo no es claro cuál es la metodología que se propone, dado que los pasos desarrollados obedecen al proceso de gestión de riesgos como tal y no a un proceso en firme de auditoria para los sistemas SCADAS.

Tabla 2.

Resumen comparativo del estado del arte.

Trabajo relacionado	Contribución	Vacíos	Proyectos propuestos
Predicción de ciberataques en sistemas industriales SCADA mediante la implementación del filtro Kalman.	Refleja la forma activa de contener ataques de seguridad	Su implementación depende de la recolección de ataques y solo se da cuando ya se fue atacado y se basa en la conformación de grupo de seguridad	Mitigar ataques de seguridad
Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA	Refleja la integridad de la metodología magerit a la exposición de un sistema scada	No implementado solo propuesto como línea de consulta	Colocar en ejecución la metodología propuesta

Nota. Esta tabla presenta el resumen comparativo a nivel teórico.

La tabla destaca dos enfoques principales para mejorar la ciberseguridad en sistemas SCADA: la predicción y contención de ciberataques mediante el filtro Kalman, y una propuesta metodológica para la auditoría de ciberseguridad basada en MAGERIT. En resumen, para fortalecer la ciberseguridad en sistemas SCADA, es fundamental combinar enfoques preventivos y reactivos, implementar metodologías de auditoría robustas y ajustar las estrategias basadas en pruebas y resultados reales.

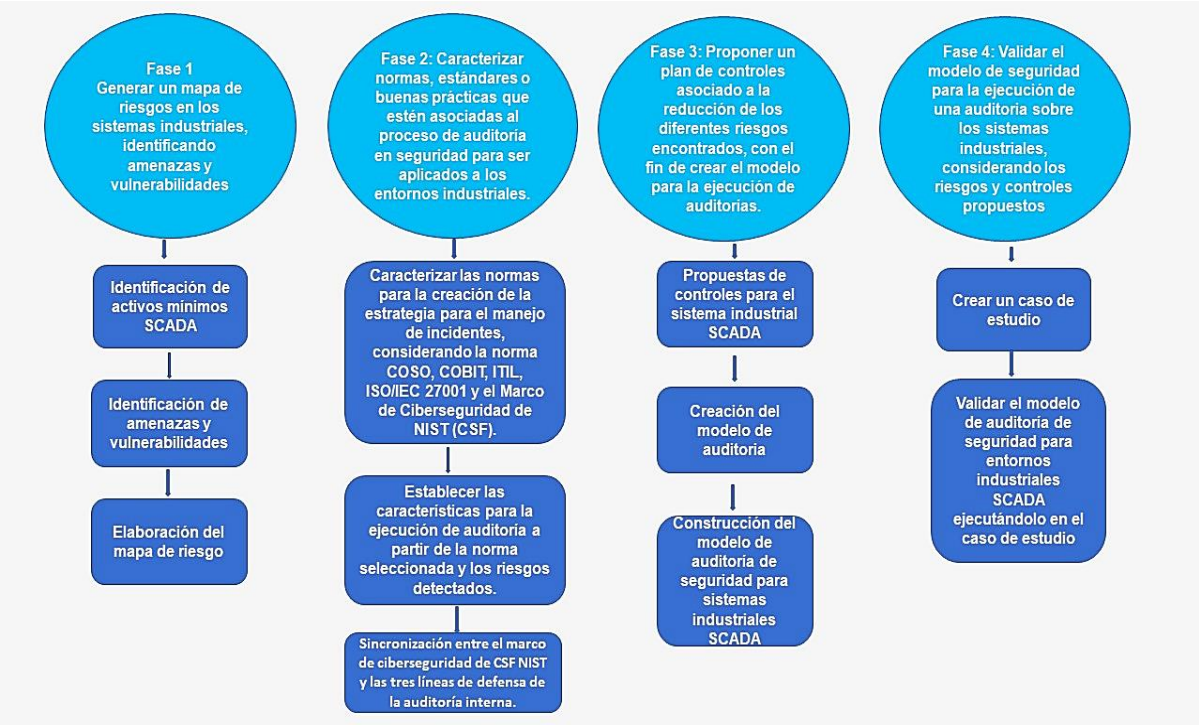
2. Metodología

La estrategia del proyecto se divide en cuatro etapas fundamentales, cada una de las cuales está cuidadosamente diseñada para lograr de manera efectiva objetivos específicos. La etapa inicial de planificación y definición de objetivos establece el rumbo del proyecto, donde se identifican y delimitan claramente los objetivos específicos. Además, se realiza una investigación exhaustiva para determinar las normas, marcos y buenas prácticas

internacionales pertinentes que servirán como guías durante el desarrollo del proyecto. Entre ellos se encuentran la ISO 27005, la ISO 19011 y el enfoque GRC (Gobierno, Riesgo, Cumplimiento), que ofrecen pautas fundamentales para la auditoría de sistemas de gestión en cuanto a la gestión de riesgos.

Figura 8.

Metodología del proyecto de investigación



Nota. Esta figura explica la metodología que se llevara a cabo de manera cronológica en el proyecto.

La figura describe un proceso metodológico completo para la auditoría de ciberseguridad en sistemas SCADA, dividido en cuatro fases interrelacionadas. Cada fase aborda un aspecto crucial del proceso de auditoría, desde la identificación de riesgos hasta la validación del modelo de seguridad.

- Fase 1: Identifica y mapea los riesgos, proporcionando una base sólida para el análisis posterior.
- Fase 2: Caracteriza las normas y estándares relevantes, alineando el proceso de auditoría con las mejores prácticas.
- Fase 3: Desarrolla y propone controles específicos para mitigar los riesgos identificados, creando un modelo de auditoría estructurado.
- Fase 4: Valida el modelo de auditoría a través de un caso de estudio, asegurando su aplicabilidad y efectividad en entornos reales.

En resumen, este proceso metodológico garantiza una evaluación exhaustiva de la ciberseguridad en sistemas SCADA, mejorando la capacidad de los sistemas industriales para resistir y responder a amenazas de seguridad.

2.1 Fase 1: Generar un mapa de riesgos en los sistemas industriales, identificando amenazas y vulnerabilidades

Esta tarea implica identificar las amenazas y vulnerabilidades que pueden afectar la integridad, disponibilidad y confidencialidad de los sistemas en entornos críticos como la infraestructura de servicios públicos, plantas de energía y otros sistemas industriales, empleando como referencia la norma ISO 27005:2018 y su procedimiento de administración correspondiente para la creación del mapa de riesgo. En resumen, este enfoque estandarizado contribuye significativamente a iniciar con la identificación de los activos críticos como las de sus amenazas y vulnerabilidades, promoviendo la resiliencia y la protección de activos esenciales.

2.1.1 Identificación de los activos mínimos de un sistema SCADA

En este punto, se ha utilizado una variedad de técnicas de consulta para realizar la identificación completa de los componentes del sistema SCADA. La búsqueda de artículos científicos y documentos disponibles tanto en bibliotecas físicas como en línea se ha utilizado para realizar la investigación bibliográfica. Además, se ha investigado activamente foros de discusión y comunidades especializadas en línea para obtener información útil sobre los sistemas SCADA. Para respaldar esta investigación, se han examinado detenidamente los manuales de usuario y la documentación técnica proporcionada por los fabricantes. Esta documentación proporciona información detallada sobre los dispositivos de entrada y salida, sensores, controladores y protocolos de comunicación utilizados en el sistema. Este proyecto es un ejercicio académico, por lo que se parte de un supuesto de controles por defecto.

El resumen de las fuentes de información seleccionadas se reportará en la etapa de resultados en la (tabla 3):

Tabla 3.

Matriz de fuentes de información seleccionadas

Item	Referencia web o tesis	Autor
1		
2		

Nota. Esta tabla presenta el formato que se utilizó para recopilar fuentes de información seleccionada en el estudio.

De esta manera gracias a la tabla anterior se logró evidenciar los activos mínimos de un sistema industrial SCADA. Para ello se reportó la información en la etapa de resultados en la mencionada a continuación en la tabla 4

Tabla 4.

Matriz activos mínimos consolidado

N°	ACTIVO	DEFINICION

Nota. Esta tabla explica la matriz de activos que fueron consolidados.

De acuerdo con la tabla 4 gracias a esta tabla se logró identificar los activos mínimos de un sistema industrial SCADA.

2.1.2 Identificación de amenazas y vulnerabilidades

La solicitud fue enviada al Center for Internet Security (CIS), una entidad sin ánimo de lucro dedicada a la seguridad de la información. CIS ofrece directrices detalladas para sistemas SCADA en su plataforma online. Se recurrió al ICS-CERT, un centro de respuesta ante riesgos de seguridad en sistemas industriales y de control, para obtener datos sobre las amenazas y vulnerabilidades más actuales en los sistemas SCADA, así como recomendaciones para mitigar estos riesgos. Además, el investigador de seguridad Matthew Luallen examinó la Base de Datos de Vulnerabilidades de SCADA, que proporciona información útil sobre fallas y exploits en los sistemas SCADA. Esta variedad de fuentes estableció una base sólida para las etapas posteriores del proyecto al consolidar una perspectiva integral de las amenazas y vulnerabilidades.

De las anteriores fuentes se recopiló una lista de amenazas y vulnerabilidades asociadas a los sistemas de infraestructura critica SCADA, eliminando los duplicados para obtener el consolidado de (5) amenazas y vulnerabilidades presentado en la tabla 5.

Tabla 5.

Listado de amenazas y vulnerabilidades consolidado

N°	AMENAZA	VULNERABILIDAD

Nota. Esta tabla explica la matriz de activos que fueron consolidados.

Esta tabla sirve para realizar una discriminación del número de amenazas y la vulnerabilidad que ocasiona.

2.1.3 Elaboración de mapa de riesgos

La identificación y evaluación de riesgos de ciberseguridad en empresas que ofrecen servicios informáticos se fundamenta en el cumplimiento de la norma ISO 27005:2018. Este estándar ofrece un marco robusto para evaluar las amenazas y vulnerabilidades dentro de estas organizaciones. A través de la implementación de los procedimientos recomendados por la norma, se logró una evaluación estructurada y completa de los riesgos. Esto incluye la identificación de activos críticos, amenazas potenciales y vulnerabilidades existentes en el entorno de las empresas de servicios informáticos.

Este enfoque basado en la norma ISO 27005:2018 permite a las organizaciones no solo reconocer los riesgos de ciberseguridad, sino también priorizarlos y desarrollar estrategias de mitigación efectivas. Al seguir los procedimientos definidos en la norma, las empresas pueden establecer un mapa de riesgos sólido que podrá servir de fundamento para la toma de decisiones informadas en materia de ciberseguridad y para la implementación de medidas preventivas y correctivas adecuadas. Este enfoque proporciona un marco confiable para abordar los desafíos de seguridad en el sector de servicios informáticos y garantizar la protección de datos y sistemas críticos.

El proceso para la creación del mapa de riesgos siguió un conjunto de etapas bien definidas, conforme a lo establecido por la normativa ISO 27005. Estas etapas implican:

1. Establecer el contexto: En este paso, se identifican los objetivos de seguridad, las partes interesadas, el alcance y las restricciones del proceso de gestión de riesgos (tabla 6).

Tabla 6.

Definición de objetivos y alcance

Definición del contexto / Alcance

Nota. Esta tabla identifica los objetivos de seguridad, las partes interesadas, el alcance y las restricciones del proceso de gestión de riesgos.

2. Identificar los activos: En este paso, se identifican los activos de información de la organización, como son los sistemas SCADA, así como los recursos que los protegen, como personal, procesos y tecnologías (tabla 7).

Tabla 7.

Componentes del sistema industrial SCADA.

ACTIVOS /RECURSOS
ACTIVO SCADA 1
ACTIVO SCADA 2
ACTIVO SCADA 3

Nota. Esta tabla describe los componentes del sistema industrial Scada.

Es esencial contar con un nivel de clasificación que permita evaluar los posibles impactos de un activo en función de su grado de importancia. Asimismo, la clasificación proporciona una perspectiva adicional, ya que el nivel de criticidad influye en la relevancia de las evaluaciones de los controles actuales y futuros (tabla 8).

La obtención de una clasificación de activos se lleva a cabo de manera semiautomatizada, considerando la importancia de cada activo en términos de posibles pérdidas, alteraciones o modificaciones en diversos aspectos. Esto resulta en una clasificación de tres niveles: Confidencial, Privada o Pública.

Tabla 8.

Clasificación de los activos vs los impactos empresariales

Activo	Afectación sobre los planes de negocio (finanzas).	Tipo de destinatario	Afecta legalmente a la empresa	Afecta las ventas o una ventaja competitiva.	Tiene afectación sobre la seguridad	Nivel de criticidad
						0 Sin clasificar

Nota. Esta tabla presenta la clasificación de los activos vs los impactos empresariales.

4. Una vez que se conoce la criticidad de cada activo y sus impactos en el negocio, se procede a identificar las vulnerabilidades asociadas y teniendo en cuenta que en este proyecto se evaluara los controles como no existentes. Este proceso tiene como objetivo mostrar los controles vigentes y proponer controles que se darán en el objetivo 3.

Tabla 9.

Clasificación de los activos vs los impactos

Activos	Vulnerabilidades	Controles actuales implementados en el activo.	Clasificación del activo	Efectividad de los controles = Eficiencia + Eficacia	0%: No se cuentan con controles implementados. 25%: Algunos controles están implementados, pero no funcionan adecuadamente o son limitados, lo que implica que no cubren completamente el riesgo identificado. 50%: Todos los controles propuestos están implementados, pero aún no se ha

	validado su efectividad. 75%: Todos los controles están implementados y se verifica su efectividad, pero no se realiza monitoreo continuo ni se elaboran planes de mejora continua. 100%: Todos los controles están implementados, se mide su efectividad mediante líneas base periódicas y auditorías, y se generan planes de acción para su mantenimiento y mejora continua.

Nota. Esta tabla presenta la clasificación de los activos vs los impactos.

5. Después de adquirir una comprensión de la situación presente, es imperativo elaborar una lista de amenazas que, en un escenario hipotético, podrían causar daños al activo mediante la explotación de las vulnerabilidades ya identificadas este proceso sienta las bases para el análisis de riesgos al cruzar escenarios potenciales.

Tabla 10.

Listado de amenazas

Listado amenazas	Factor de riesgos

Nota. Esta tabla presenta la clasificación de listado de amenazas y factor de riesgos.

6. Ahora bien, este apartado se centró en los escenarios de riesgo que son una herramienta fundamental en la gestión de riesgos de seguridad de la información, ya que permiten a las organizaciones visualizar y evaluar cómo las amenazas pueden impactar sus activos críticos, lo que a su vez facilita la toma de decisiones orientadas a la seguridad y la continuidad del negocio.

Tabla 11.

Amenazas Vs Activos

ACTIVOS **AMENAZAS**		

Nota. Esta tabla presenta la clasificación de activos Vs amenazas.

7. Con esta comprensión, se buscó explorar las posibles situaciones de riesgo con el propósito de evaluar su impacto. Los indicadores de impacto deben ser elaborados y detallados en relación con el grado de perjuicio o gastos que un riesgo de seguridad de la información podría ocasionar a la empresa. Un enfoque empresarial del impacto se utiliza para cuantificar las repercusiones.

Para identificar las situaciones de riesgo, se efectuó un análisis sobre cómo estas afectarían a la organización. La valoración se debe adaptar según el tipo de empresa y sus principios corporativos, considerando qué factores podrían tener un impacto más significativo en sus procesos centrales si fueran afectados. Dado que la seguridad de la información se ha vuelto un componente integral de los valores corporativos en muchas organizaciones debido a la convergencia tecnológica, esto podría ser un punto de partida para evaluar las implicaciones.

El presente estudio se enfoca en la evaluación del impacto teniendo en cuenta la probabilidad de ocurrencia (según se detalla en la (tabla 12) en contraposición al impacto en la disponibilidad (como se describe en la (tabla 13). Esta aproximación se adopta debido a que las organizaciones de infraestructura critica están expuestas a su funcionamiento y reputación y dado que la información puede ser sensible para el trabajo desempeñado.

Tabla 12.

Probabilidad o Frecuencia

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Raro**	Puede ocurrir solo bajo circunstancias excepcionales
2	**Improbable**	Podría ocurrir algunas veces
3	**Posible**	Puede ocurrir en algún momento
4	**Probable**	Probabilidad de ocurrencia en la mayoría de las circunstancias
5	**Casi seguro**	La expectativa de ocurrencia se da en la mayoría de las circunstancias

Nota. Esta tabla presenta la clasificación de rangos y su descripción.

La tabla proporciona una estructura clara para evaluar la probabilidad de ocurrencia de eventos en sistemas y procesos, lo que es crucial para la gestión de riesgos. Cada nivel define con precisión la frecuencia esperada, permitiendo a los gestores de riesgos y a los ingenieros de sistemas priorizar las acciones preventivas y correctivas según la probabilidad de los eventos.

Tabla 13.

Impacto en la información pilar disponibilidad

Nivel	Rangos	Ejemplo detallado de la descripción
1	**Insignificante**	Hay una indisponibilidad menor a 30 min y la puede resolver la mesa de ayuda. O,
2	**Menor**	Hay una indisponibilidad entre 1 y 2 horas, es necesario escalarlo a 2 nivel
3	**Intermedio**	Hay una indisponibilidad entre 2 y 4 horas, se requiere consulta el proveedor
4	**Mayor**	Hay una indisponibilidad entre 4 y 8 horas, se requiere al proveedor en sitio.
5	**Superior**	Hay una indisponibilidad por más de 12 horas, es necesario establecer un mecanismo de procesamiento alterno.

Nota. Esta tabla presenta la clasificación de rangos y su descripción.

8. Utilizando el entendimiento adquirido mediante la identificación de las variables mencionadas, se inicia un proceso de evaluación que generará un informe que mostrará la situación presente y las posibles repercusiones en una organización (teniendo en cuenta los controles son inexistentes). Del mismo modo, se determinará el grado de impacto en términos del conocimiento en caso de que el activo sea comprometido. Para llevar a cabo esta evaluación, se establecen los parámetros definidos en la tabla que se presenta a continuación.

Tabla 14. *Impacto en la operatividad - disponibilidad*

No.	Escenario de riesgos	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto Cliente Mercado	Clasificación del activo

Nota. Esta tabla presenta los diferentes escenarios de riesgos.

9. Para evaluar de manera integral los niveles de riesgo, se implementa una matriz de criticidad de 5x5. Esta herramienta proporciona una visión detallada al asignar cinco niveles tanto para la probabilidad como para el impacto de los eventos adversos. Al utilizar esta matriz, se logra una clasificación más precisa de los riesgos, permitiendo una identificación efectiva de las amenazas críticas y facilitando la toma de decisiones informadas para la mitigación de estos. La estructura de 5x5 asegura una evaluación robusta y sistemática,

mejorando la comprensión global de los riesgos y contribuyendo a un enfoque proactivo en la gestión de la seguridad.

Tabla 15.

Matriz de Riesgos

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3					
Improbable	2					
Raro	1					

Nota. Esta tabla presenta la probabilidad y consecuencias en una matriz de riesgo

Las regiones en el mapa de riesgos se dividen de la siguiente manera:

- Zona Verde: Categorizada como una zona de riesgo aceptable.
- Zona Amarilla: Designada como una zona de riesgo tolerable.
- Zona Naranja: Identificada como una zona de riesgo inadmisible.
- Zona Roja: Clasificada como una zona de riesgo inaceptable.

Los riesgos que poseen una alta probabilidad y un impacto significativo reciben una mayor atención y se ubican en las zonas naranja y roja. Estos riesgos son los que se someterán a un plan de tratamiento y mitigación. En contraste, los riesgos en las zonas de menor riesgo (verde y amarillo) se consideran aceptables y no requerirán acciones inmediatas de tratamiento.

El sustento para la elaboración de la matriz de riesgos conforme al cumplimiento de la norma ISO 27005:2018 proporciona un marco sólido para la identificación, evaluación y gestión de riesgos de ciberseguridad. Esta norma establece un enfoque sistemático y riguroso para abordar los desafíos de seguridad, garantizando la protección de datos y sistemas críticos.

En lo que respecta a los sistemas industriales, como los sistemas de control y adquisición de datos (SCADA), son componentes esenciales en diversas industrias, controlando procesos críticos como la distribución de energía, el tratamiento de agua y el transporte de petróleo y gas. La complejidad y la interconexión de estos sistemas los hacen vulnerables a una amplia gama de amenazas, lo que hace que la creación de un mapa de riesgos sea una herramienta fundamental para la gestión de la seguridad.

La elaboración del mapa de riesgos para sistemas industriales se basará en dos normas internacionales clave:

ISO 27001:2013 - Sistemas de gestión de la seguridad de la información:

- Proporciona un marco general para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en cualquier organización.
- Establece los requisitos para identificar, evaluar y tratar los riesgos de seguridad de la información, incluyendo aquellos relacionados con los sistemas industriales.

IEC 62443 - Seguridad industrial - Ciberseguridad para sistemas de control y adquisición de datos (ICS):

- Se enfoca específicamente en la seguridad de los sistemas industriales, proporcionando directrices para la implementación de medidas de seguridad en estos entornos.
- Complementa la norma ISO 27001 con requisitos y recomendaciones específicas para la gestión de riesgos de ciberseguridad en ICS.

Sustento de la Investigación para el Mapa de Riesgos

La investigación para la elaboración del mapa de riesgos en sistemas industriales bajo el marco de ISO 27001 e IEC 62443 se basará en los siguientes aspectos:

Identificación de Activos:

- Inventario exhaustivo de activos ICS: Realizar un inventario completo de todos los activos del sistema industrial, incluyendo hardware, software, redes de comunicación, datos y personal.
- Clasificación de activos según la criticidad: Clasificar los activos ICS en función de su impacto potencial en la seguridad y la operación del sistema, considerando factores como la severidad de una falla o interrupción.
- Análisis de dependencias entre activos: Identificar las dependencias entre los activos ICS para comprender cómo un riesgo en un activo podría afectar a otros.

Análisis de Amenazas y Vulnerabilidades:

- Identificación de amenazas internas y externas: Considerar una amplia gama de amenazas potenciales para los sistemas industriales, como errores humanos, ataques cibernéticos, desastres naturales, sabotaje y fallas de equipos.
- Evaluación de la probabilidad de ocurrencia: Estimar la probabilidad de que cada amenaza se concrete, considerando factores como el historial de ataques, las vulnerabilidades del sistema y las medidas de seguridad existentes.

- Identificación de vulnerabilidades en los activos ICS: Examinar los activos del sistema industrial para identificar debilidades que podrían ser explotadas por las amenazas.

- Evaluación del impacto de las vulnerabilidades: Estimar el impacto potencial que cada vulnerabilidad podría tener en los activos ICS, considerando la severidad de la explotación y la criticidad de los activos afectados.

Cálculo del Riesgo:

- Fórmula de riesgo ISO 27001: Utilizar la fórmula de riesgo establecida en la norma ISO 27001:2013, que considera el impacto potencial (P) y la probabilidad de ocurrencia (O) de cada amenaza-vulnerabilidad.

- Cálculo del riesgo para cada activo ICS: Calcular el riesgo individual para cada activo ICS, considerando las amenazas y vulnerabilidades que lo afectan.

- Priorización de riesgos: Priorizar los riesgos en función de su valor, enfocando los esfuerzos de mitigación en aquellos que representan el mayor peligro para la seguridad y la operación del sistema industrial.

Definición de Controles de Seguridad:

- Controles preventivos: Identificar e implementar controles preventivos para reducir la probabilidad de ocurrencia de riesgos de seguridad en los sistemas industriales, como firewalls, autenticación, cifrado, segmentación de redes y capacitación del personal en ciberseguridad industrial.

- Controles correctivos: Identificar e implementar controles correctivos para minimizar el impacto y la recuperación en caso de que ocurra un riesgo de seguridad en los sistemas industriales, como planes de respuesta a riesgos, procedimientos de recuperación de desastres y análisis forense digital.

- Asignación de controles a activos y riesgos: Asignar los controles de seguridad identificados a los activos ICS y riesgos específicos que requieren protección.

2.2 Fase 2: Caracterizar normas, estándares o buenas prácticas que estén asociadas al proceso de auditoría en seguridad para ser aplicados a los entornos industriales

En el contexto de una auditoría basada en la gestión de riesgos, el objetivo es examinar las normativas pertinentes para la elaboración de estrategias de gestión de riesgos. Entre las normas que revisten interés se encuentran COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF).

Identificar los elementos clave de cada norma desempeña un papel fundamental en la evaluación de su adaptabilidad y aplicabilidad en un contexto de auditoría. Se ha realizado una comparación detallada de estas normas mediante la utilización de criterios fundamentales que facilitan la comprensión de sus características distintivas.

2.2.1 Caracterizar las normas para la creación de la estrategia para gestión de riesgos, considerando la norma COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF)

En el ámbito de una auditoría, las ventajas inherentes a cada norma se encuentran ligadas a los aspectos destacados en su enfoque, especialmente aquellos que guardan relación con los procedimientos documentados para su correcta implementación. Estos procedimientos constituyen descripciones detalladas de los pasos y procesos presentes en la documentación de cada marco normativo, siendo elementos esenciales para lograr una implementación eficaz y acorde a los estándares establecidos.

Un concepto de relevancia fundamental reside en el enfoque intrínseco de cada norma; algunas se enfocan en la seguridad de la información en su totalidad, mientras que otras adoptan un enfoque más específico, centrado en la ciberseguridad. La elección de la norma adecuada durante una auditoría dependerá directamente de los objetivos y requisitos específicos de la organización en relación con la seguridad y la gestión de riesgos, asegurando así una evaluación efectiva y alineada con los estándares normativos y las necesidades particulares de la entidad auditada.

Tabla 16.

Normas y definición criterios

	Ventajas	Procesos	Enfoque
COSO			
COBIT			
ITIL			
ISO/IEC 27001			
Marco de Ciberseguridad de NIST (CSF)			

Nota. Esta tabla presenta los diferentes criterios de las normas.

Una vez que se han determinado las normas y sus características, se procede a verificar la siguiente actividad, que se enmarca en la estrategia para la selección de la norma.

No obstante, se considera importante destacar que efectivamente, no tiene sentido partir de la Gestión de Riesgos para definir el modelo para la ejecución de auditorías de seguridad en sistemas industriales SCADA. Puesto que las auditorías de seguridad y la gestión de riesgos son dos procesos distintos con objetivos y enfoques diferentes tal como se explica a continuación:

Auditorías de seguridad:

- Objetivo: Evaluar la postura de seguridad actual de un sistema o entorno para identificar vulnerabilidades, riesgos y deficiencias en los controles de seguridad.

- Enfoque: Proactivo, preventivo y orientado a la identificación de problemas potenciales antes de que ocurran riesgos.
- Metodología: Basada en la evaluación de riesgos, el análisis de controles y la verificación del cumplimiento de normas y estándares.

Gestión de riesgos:

- Objetivo: Responder a riesgos de seguridad que ya han ocurrido, minimizando su impacto y restaurando la normalidad lo antes posible.
- Enfoque: Reactivo, correctivo y orientado a la contención, investigación y recuperación de riesgos.
- Metodología: Basada en la detección, el análisis, la contención, la erradicación, la recuperación y el aprendizaje.

Por lo tanto, partir de la Gestión de Riesgos para definir el modelo de auditoría tendría las siguientes desventajas:

- Enfoque reactivo: Se enfocaría en problemas ya ocurridos, en lugar de prevenir futuros riesgos.
- Limitación del alcance: Se concentraría en los riesgos detectados, omitiendo otras vulnerabilidades y riesgos potenciales.
- Falta de visión preventiva: No permitiría una evaluación integral de la postura de seguridad del sistema.
- Metodología inadecuada: La metodología de gestión de riesgos no está diseñada para identificar y evaluar riesgos de manera sistemática.

En cambio, el modelo de auditoría de seguridad debe basarse en una metodología proactiva y preventiva que permita:

- Identificar vulnerabilidades y riesgos: Antes de que puedan ser explotados por actores maliciosos.
- Evaluar la efectividad de los controles de seguridad: Para garantizar que sean adecuados y brinden la protección necesaria.
- Verificar el cumplimiento de normas y estándares: Para demostrar que el sistema cumple con los requisitos mínimos de seguridad.
- Detectar deficiencias en las prácticas de seguridad: Para tomar medidas correctivas y mejorar la postura de seguridad general.

En resumen, la Gestión de Riesgos es un componente importante de la seguridad, pero no debe ser el punto de partida para definir el modelo de auditoría de seguridad en sistemas SCADA. La auditoría debe enfocarse en la evaluación preventiva de riesgos y controles para fortalecer la postura de seguridad y prevenir riesgos futuros.

Teniendo en cuenta lo anterior, se considera que el enfoque Correcto para la Auditoría de Seguridad en Sistemas Industriales SCADA, se fundamenta en los siguientes elementos:

- Partida: La definición del modelo de auditoría de seguridad en sistemas SCADA no debe basarse en la Gestión de Riesgos.

- Énfasis: La auditoría debe enfocarse en la evaluación preventiva de riesgos y controles de seguridad, con el objetivo de identificar vulnerabilidades y deficiencias antes de que ocurran riesgos.

- Metodología: Utilizar una metodología estructurada basada en normas y estándares como ISO/IEC 27001, IEC 62443, ISO 19001, NIST SP 800-53 e ISA/IEC 62853, junto con buenas prácticas como SANS 918 Industrial Control System Security, ISA Secure, CIS Critical Security Controls (CSC) for ICS y el Marco de Ciberseguridad de NIST (CSF).

- Alcance: La auditoría debe abarcar todos los aspectos de la seguridad del sistema SCADA, incluyendo:
    - Identificación de activos: Inventario completo de todos los componentes del sistema, incluyendo hardware, software, redes y datos.
    - Análisis de amenazas y vulnerabilidades: Evaluación de las amenazas potenciales y las vulnerabilidades existentes en el sistema.
    - Evaluación de riesgos: Cálculo del riesgo asociado a cada amenaza-vulnerabilidad.
    - Análisis de controles: Evaluación de la efectividad de los controles de seguridad implementados para mitigar los riesgos.
    - Verificación del cumplimiento: Verificación del cumplimiento de las normas, estándares y buenas prácticas de seguridad.

- Resultados: La auditoría debe generar un informe detallado que incluya:
    - Hallazgos identificados, incluyendo vulnerabilidades, deficiencias en los controles y riesgos potenciales.
    - Priorización de los hallazgos en función de su severidad e impacto potencial.
    - Recomendaciones para la mitigación de los riesgos y la mejora de la postura de seguridad del sistema SCADA.

Beneficios:

- Prevención de riesgos: La identificación y mitigación proactiva de riesgos reduce la probabilidad de que ocurran riesgos de seguridad.

- Protección de activos críticos: La auditoría permite proteger los activos críticos del sistema SCADA contra amenazas internas y externas.

- Cumplimiento normativo: El cumplimiento de las normas y estándares de seguridad garantiza la confiabilidad y la integridad del sistema.
- Mejora continua de la seguridad: La auditoría fomenta una cultura de seguridad y la mejora continua de la postura de seguridad del sistema SCADA.

En definitiva, partir de la evaluación de riesgos y controles de seguridad de la información y ciberseguridad, excluyendo la gestión de riesgos, es el enfoque correcto para definir el modelo de auditoría de seguridad en sistemas industriales SCADA. Además, este enfoque garantiza una estrategia proactiva y preventiva para identificar y abordar los riesgos de seguridad, proteger los activos críticos y mejorar la postura general de seguridad de estos sistemas críticos.

2.2.2 Establecer las características para la ejecución de auditoría a partir de la norma seleccionada y los riesgos altos detectados

Esta metodología tuvo como objetivo principal establecer la estrategia para llevar a cabo una auditoría, partiendo del objetivo general que se enfoca en la creación de un modelo de auditoría de seguridad para sistemas industriales SCADA.

Para elegir, definir o agrupar las metodologías pertinentes, se consideró los siguientes criterios. Esto se hizo teniendo en mente que se trata de una propuesta dirigida a empresas de infraestructura crítica y es esencial identificar y comprender los elementos fundamentales como son:

Documentación: La importancia de la documentación dentro del contexto de una norma radica en ofrecer directrices claras y concisas para la elaboración de registros, procedimientos, políticas y cualquier otro tipo de documentación requerida para la implementación y el cumplimiento de los requisitos establecidos por la norma. La documentación no solo sirve como una guía para los profesionales involucrados, sino que también es esencial para mantener un registro de las actividades y decisiones relevantes. Esto puede incluir la creación de manuales de procedimientos, informes de auditoría, registros de riesgos y otros documentos que ayuden a garantizar la coherencia y la calidad en la aplicación de la norma.

Auditable: La auditabilidad se refiere a la capacidad de una norma para someterse a procesos de auditoría, lo que significa que es posible evaluar y verificar el cumplimiento de sus requisitos. Esto implica que la norma debe estar diseñada de tal manera que sus requisitos sean medibles, verificables y que existan métodos claros para la evaluación. La auditabilidad es esencial para garantizar la confianza en el cumplimiento de la norma y puede involucrar la revisión de registros, entrevistas con personal, inspecciones de sistemas y otros procedimientos para verificar que se están siguiendo los estándares establecidos.

Auditable para Ciberseguridad: Dentro del ámbito de los sistemas SCADA (Supervisory Control and Data Acquisition), la ciberseguridad abarca la implementación de medidas de seguridad diseñadas para proteger estos sistemas contra ciberataques y amenazas informáticas. Las normas que incluyen requisitos de ciberseguridad buscan garantizar la

integridad, la confidencialidad y la disponibilidad de los datos y sistemas SCADA, ya que estos sistemas suelen ser críticos para el funcionamiento de infraestructuras clave, como redes eléctricas y plantas industriales. Las medidas de ciberseguridad pueden incluir la segmentación de redes, la autenticación de usuarios, la detección de intrusiones y la gestión de vulnerabilidades, entre otras estrategias para prevenir y responder a posibles ataques cibernéticos.

Auditable para Sistemas SCADA: La audibilidad de una norma en relación con los sistemas SCADA se refiere a la capacidad de esta norma para ser utilizada como una referencia que permite evaluar y verificar el cumplimiento de sus requisitos en los sistemas de Supervisory Control and Data Acquisition (SCADA) que una organización utiliza. Esta audibilidad no se limita a simplemente aplicar la norma a ciegas, sino que implica un proceso reflexivo y estratégico por parte de la organización para determinar si los estándares establecidos en la norma son adecuados y relevantes para sus sistemas SCADA específicos.

Fácil Implementación para Sistemas SCADA: La facilidad de implementación en sistemas SCADA se refiere a la capacidad de aplicar los requisitos y estándares de una norma de manera eficiente y efectiva en el entorno de los sistemas de Supervisory Control and Data Acquisition (SCADA) de una organización. Esta característica es fundamental para garantizar que los sistemas SCADA cumplan con los estándares de seguridad, operatividad y gestión de riesgos de manera viable y sin generar una carga excesiva de trabajo.

Tabla 17.

Normas y calificación criterios

Criterios Normas	Documentación	Auditable	Auditable para ciberseguridad	Auditable para sistema SCADA	Fácil implementación para sistemas SCADA
COSO					
COBIT					
ITIL					
ISO/IEC 27001					
Marco de Ciberseguridad de NIST (CSF)					

Nota. Esta tabla presenta los diferentes criterios de las normas.

La norma que se elija será aquella que obtenga la puntuación más alta. En situaciones donde las calificaciones sean iguales al sumar los puntajes, se requerirá examinar si esa igualdad se relaciona con la complementariedad entre las normativas.

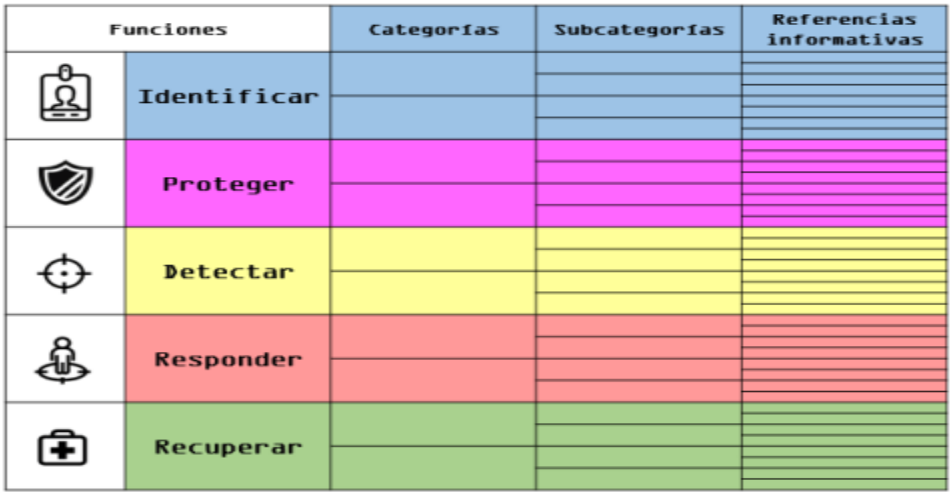
2.2.3 Sincronización entre el marco de ciberseguridad de CSF NIST y las tres líneas de defensa de la auditoría interna

Esta actividad proporcionó el conocimiento previo tanto del CSF NIST como de la auditoría, fundamentales para la creación del modelo de ejecución de auditoría de seguridad en entornos industriales SCADA. La explicación detallada aborda los tres componentes y sus atributos, junto con su integración en las tres líneas de defensa de la auditoría interna. Con el propósito de comprender la estructura del marco de ciberseguridad del NIST, que se utiliza como buena práctica para alcanzar el objetivo general, desglosandolo, explicando cada uno de sus componentes, como el Marco Básico, los Niveles de Madurez y los Perfiles del Marco. El Marco Básico se destaca como la parte central y fundamental del marco, diseñado para proporcionar una estructura y un lenguaje comunes para la gestión de la ciberseguridad. Contiene funciones, categorías y subcategorías que guían a las organizaciones en la identificación, protección, detección, respuesta y recuperación de amenazas cibernéticas.

En el análisis detallado de la actividad, se desentrañan los conocimientos previos sobre el CSF NIST y la auditoría, esenciales para la creación del modelo de ejecución de auditoría de seguridad en entornos industriales SCADA. Los tres componentes y sus atributos se explican en relación con su integración en las tres líneas de defensa de la auditoría interna. Para obtener una comprensión integral de la estructura del marco de ciberseguridad del NIST, utilizado como buena práctica para alcanzar el objetivo global, se realiza un desglose detallado de sus componentes, incluidos el Marco Básico, los Niveles de Madurez y los Perfiles del Marco. El Marco Básico, siendo la parte central y fundamental, se diseñó para proporcionar una estructura y un lenguaje comunes para la gestión de la ciberseguridad, incorporando funciones, categorías y subcategorías que asisten a las organizaciones en la identificación, protección, detección, respuesta y recuperación de amenazas cibernéticas.

Figura 9.

Estructura del marco básico del CSF.



Nota. Esta figura muestra el marco básico del CSF del NIST. *Fuente: tomado de* [56]

La figura representa la estructura del marco básico del Cybersecurity Framework (CSF) del Instituto Nacional de Estándares y Tecnología (NIST). El CSF se organiza en cinco funciones esenciales que abordan distintos aspectos de la gestión de la ciberseguridad. Cada función se descompone en categorías y subcategorías, con referencias informativas que guían su implementación.

Los Niveles de Madurez ofrecen una evaluación del progreso de una organización en la implementación del marco de ciberseguridad, abarcando desde el Nivel 1 (Inicial) hasta el Nivel 4 (Adaptativo). Cada nivel representa un aumento progresivo en sofisticación y madurez en la gestión de la ciberseguridad. A medida que una organización avanza a través de los niveles, demuestra una mayor eficacia en la gestión de riesgos y amenazas cibernéticas. Estos niveles proporcionan una herramienta valiosa para medir la capacidad actual de una organización y establecer objetivos claros para mejorar su postura de ciberseguridad. Con un enfoque ascendente en los Niveles de Madurez, las organizaciones pueden trazar un camino estructurado hacia la mejora continua, fortaleciendo su resiliencia ante las amenazas digitales en un entorno cada vez más complejo y dinámico.

Figura 10.

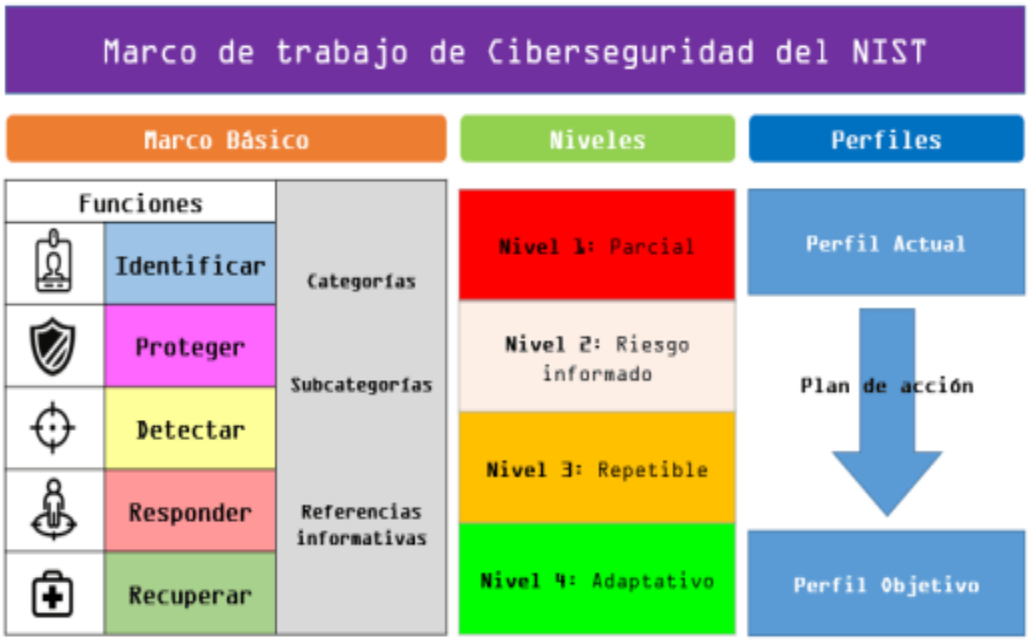
Niveles de Implementación

Nota. Esta figura muestra un diagrama de los niveles de un marco de trabajo de ciberseguridad para la gestión de riesgos de ciberseguridad en organizaciones.

Los Perfiles del Marco brindan a las organizaciones la capacidad de personalizar la implementación del marco de ciberseguridad según sus necesidades específicas y objetivos. Estos perfiles consisten en conjuntos seleccionados de categorías y subcategorías del Marco Básico, junto con objetivos específicos y requisitos organizativos. Esta flexibilidad permite a las organizaciones adaptar el marco a sus circunstancias únicas, como su industria, su entorno de amenazas y sus recursos disponibles. La creación de un perfil permite a una organización centrarse en las áreas críticas de ciberseguridad que son más relevantes para sus operaciones y riesgos, facilitando una implementación más efectiva y eficiente del marco en función de sus necesidades particulares. Siguiendo las explicaciones previas, la estructura general del marco de ciberseguridad se presentaría de la siguiente manera (Figura 11).

Figura 11.

Arquitectura del marco de trabajo de ciberseguridad del NIST (CSF).



Nota. Esta figura muestra ciberseguridad del NIST (CSF). *Fuente: Tomado de.* [56]**.**

En conjunto, el Marco Básico, los Niveles de Madurez y los Perfiles del Marco forman una estructura robusta y adaptable que permite a las organizaciones diseñar y mejorar sus programas de ciberseguridad. El Marco Básico, al proporcionar una base común, establece los principios fundamentales necesarios para gestionar la ciberseguridad de manera integral. Los Niveles de Madurez ofrecen una medida escalonada del progreso, permitiendo a las organizaciones evaluar su capacidad y establecer metas de mejora. Por su parte, los Perfiles del Marco ofrecen la flexibilidad necesaria para adaptar el marco a las necesidades y circunstancias específicas de cada organización, permitiendo una personalización precisa. Esta combinación integral proporciona a las organizaciones las herramientas esenciales para alinear sus programas de ciberseguridad con sus necesidades particulares y las mejores prácticas del sector, fomentando un enfoque robusto y eficaz ante las amenazas digitales.

Una vez desarrollada la actividad anterior, se procedió a implementar este marco tanto en ciberseguridad como en auditoría. Durante este proceso, se identificó la necesidad de proporcionar algunos conceptos adicionales para mejorar su comprensión, que incluyen los siguientes:

Ciberseguridad se refiere a la protección de activos de información contra amenazas que puedan comprometer la integridad, confidencialidad y disponibilidad de la información procesada, almacenada y transportada por sistemas interconectados. En este contexto, la capacidad de recuperación rápida es crucial; por lo tanto, no se trata tanto de evitar caídas como de levantarse rápidamente. En este sentido, la convergencia e interacción efectiva entre

las tres líneas de defensa son fundamentales para proporcionar a las organizaciones herramientas efectivas para prevenir y minimizar el impacto de los riesgos de seguridad.

La integración del modelo de 3 líneas de defensa (ver Figura 12) ha sido fundamental, armonizando la auditoría con el framework de ciberseguridad de la NIST. Este proceso conceptual ha contribuido de manera significativa al desarrollo de la metodología, como se detalla en el punto 4.2.3. La sinergia entre el modelo de 3 líneas de defensa y el framework de ciberseguridad de la NSIT ha permitido una alineación precisa, fortaleciendo la capacidad conceptual para abordar la metodología propuesta. Este enfoque integrado no solo mejora la comprensión de los procedimientos de auditoría, sino que también potencia la eficacia y eficiencia de la implementación del marco de ciberseguridad. La colaboración armoniosa de estos elementos clave proporciona una base sólida para el diseño y la ejecución de procesos de auditoría que están intrínsecamente alineados con las mejores prácticas de ciberseguridad y los estándares establecidos por la NIST.

Figura 12.

Modelo de 3 líneas de defensa adaptado a ciberseguridad

Nota. Esta figura muestra el modelo de las tres líneas de defensa para la gestión de riesgos de ciberseguridad. *Fuente: tomado de [33].*

La gestión efectiva de riesgos en ciberseguridad se erigió como una piedra angular para preservar los activos digitales y la integridad organizativa en un entorno cada vez más interconectado. En este dinámico escenario, se desplegó de manera óptima el modelo de las

tres líneas de defensa, proporcionando un marco integral para abordar y mitigar los riesgos inherentes a la ciberseguridad.

La primera línea de defensa, focalizada en las partes operativas de la organización, engloba a los empleados y equipos directamente involucrados en la ejecución de actividades y procesos. Su función principal radica en la gestión proactiva y el control efectivo de los riesgos dentro de sus respectivas áreas de responsabilidad, constituyendo así el primer frente de defensa ante amenazas cibernéticas.

La segunda línea de defensa amplía su alcance hacia las funciones de gestión de riesgos y cumplimiento en la organización. Estas funciones desempeñan un papel crucial al supervisar y respaldar la gestión de riesgos en la primera línea, asegurando la coherencia con las políticas y regulaciones establecidas para fortalecer aún más la postura de ciberseguridad de la organización.

La tercera línea de defensa, representada por las unidades de auditoría interna o auditorías independientes, desempeña un papel esencial en este contexto. Su misión es proporcionar una evaluación independiente y objetiva de los controles y procesos en toda la organización. Al hacerlo, aseguran que tanto la gestión de riesgos como el control interno operen de manera eficaz y estén alineados con los estándares más rigurosos de ciberseguridad. Estas unidades de auditoría desempeñan un papel crucial en garantizar la resiliencia del sistema de ciberseguridad y la mitigación efectiva de amenazas potenciales [57].

En última instancia, el modelo de las tres líneas de defensa, adaptado al riesgo de ciberseguridad, ha proporcionado una estructura robusta y cohesionada para gestionar de manera efectiva y mitigar los riesgos en un entorno digital que evoluciona constantemente. Cada línea, desde la primera hasta la tercera, ha desempeñado un papel vital en resguardar los activos digitales y prevenir posibles brechas de seguridad cibernética que podrían haber tenido consecuencias significativas para la organización. Este enfoque holístico ha demostrado ser esencial en la protección proactiva y la respuesta efectiva a los desafíos emergentes en el panorama de la ciberseguridad.

Al comprender a fondo el enfoque de las tres líneas de defensa adaptado a los riesgos de ciberseguridad, se facilita una armonización estratégica con el marco de ciberseguridad del NIST. Esta sincronización se refleja específicamente en la Tabla 18, que detalla la implementación del framework y las tres líneas de defensa. Esta integración proporciona un marco integral y coherente para la gestión de riesgos cibernéticos, asegurando la alineación con las mejores prácticas y estándares reconocidos en el ámbito de la ciberseguridad [58].

Tabla 18.

Acople del marco CSF y las 3 líneas de defensa de auditoria

FASE	CATEGORIA	IMPLEMENTACION DEL FRAMEWORK CSF NIST			POST IMPLEMENTACION	
		1a línea de defensa	2a línea de defensa	3a línea de defensa	Auditoria	Auditoria continua
Identificar	Gestión de activos					
	Ambiente de negocios					
	Gobernanza					
	Evaluación de riesgos					
	Estrategia de gestión de riesgos					
	Gestión de riesgos de la cadena de suministro					
Proteger	Gestión de identidad, autenticación y Control de acceso					
	Concienciación y capacitación					
	Seguridad de los datos					
	Procesos y procedimientos de protección de la información					
	Mantenimiento					
	Tecnología de protección					
Detectar	Anomalías y eventos					
	Monitoreo continuo de seguridad					
	Procesos de detección					
Responder	planificación de Respuestas					
	Comunicaciones					
	Análisis					
	Mitigación					
	Mejoras					
Recuperar	Planificación de la recuperación					
	Mejoras					
	Comunicaciones					

Nota. La tabla resume las diferentes fases y categorías del marco NIST Cybersecurity Framework (CSF) en el contexto de la implementación y post-implementación en una organización.

La fusión de estas dos metodologías ha culminado en un proceso que ha generado sinergia, traduciéndose en una notable mejora en la eficiencia y precisión de nuestras auditorías de seguridad. Este enfoque integrado ha fortalecido nuestra capacidad para identificar y mitigar de manera efectiva los riesgos técnicos en nuestros sistemas SCADA. La confianza resultante en nuestras capacidades de gestión de riesgos ha experimentado un aumento significativo, ya que ahora se cuenta con un enfoque de auditoría más robusto y adaptado a las cambiantes necesidades del entorno industrial. Este proceso de integración ha demostrado ser fundamental para mantener la seguridad y la integridad de los sistemas en un entorno en constante evolución.

2.3 Fase 3: Proponer un plan de controles asociado a la reducción de los diferentes riesgos encontrados, con el fin de crear el modelo para la ejecución de auditorías

En el marco del proyecto de evaluación y mejora de la seguridad en las infraestructuras críticas (ICS) las cuales se utilizan sistemas industriales SCADA, se propone el proceso de gestión de riesgos enfocado en la norma ISO 27005. Durante esta revisión, se identifican varias amenazas y vulnerabilidades en los sistemas y procesos críticos de la organización generando riesgos potenciales. Estas evidencias resaltan la necesidad urgente de implementar medidas de seguridad efectivas para proteger la infraestructura y garantizar su funcionamiento ininterrumpido.

Con el propósito de hacer frente a los riesgos claramente identificados y elevar la resiliencia de los sistemas industriales, se plantea la necesidad imperante de formular un plan integral de controles de seguridad. Este plan esta diseñado con el objetivo específico de mitigar los riesgos previamente identificados, estableciendo así las bases para un entorno operativo que no solo sea más seguro, sino también más robusto y resistente frente a posibles amenazas. Este enfoque estratégico no solo busca abordar los riesgos de manera proactiva, sino también promover una cultura de seguridad sostenible que respalde la continuidad operativa y la protección continua de los activos críticos.

El objetivo final de esta iniciativa es desarrollar un modelo detallado y efectivo para llevar a cabo auditorías de seguridad en sistemas SCADA. Este modelo se fundamenta en un plan de controles meticulosamente diseñado y adaptado a las necesidades particulares de la organización. Además, servirá como guía para auditorías futuras y asegurará un enfoque sistemático y coherente en la gestión de riesgos y la seguridad dentro del entorno industrial. Durante esta fase se adelantan (2) actividades principales que se relacionan a continuación.

2.3.1 Propuestas de controles para el sistema industrial SCADA

El propósito de esta sección es proporcionar al proyecto una guía clara y detallada sobre las acciones que deben llevarse a cabo para fortalecer la seguridad de los sistemas SCADA. Cada propuesta de control se diseña con el objetivo de mejorar la resiliencia de los sistemas y garantizar que se cumplan los estándares de seguridad requeridos. Estas recomendaciones se convierten en la base para la planificación y la implementación de medidas de seguridad efectivas en el entorno de sistemas SCADA, con el fin de proteger los activos críticos de la

organización y mantener la integridad de sus operaciones industriales. El estándar del NIST especifica cinco elementos fundamentales dentro de su Marco de Referencia.

Figura 13.

Controles marco del NIST

ID	**Identificar**	Gestión de activos
		Entorno de negocio
		Gobernanza
		Evaluación de riesgos
		Gestión de riesgos
		Gestión de riesgos de la cadena de suministro
PR	**Proteger**	Gestión de identidades y control de acceso
		Concienciación y formación
		Seguridad del dato
		Procesos de protección de la información y procedimientos
		Mantenimiento
		Tecnologías de protección
DE	**Detectar**	Anomalías y eventos
		Monitorización continua de la seguridad
		Procesos de detección
RS	**Responder**	Planificación de la respuesta
		Comunicaciones
		Análisis
		Mitigación
		Mejoras
RC	**Recuperar**	Planificación de la recuperación
		Mejoras
		Comunicaciones

Nota. La figura muestra las etapas de los controles NIST. *Fuente: tomado* de **[59]**.

Los controles seleccionados se reportarán en la etapa de resultados en la tabla 18:

Tabla 19.

Controles propuestos

Numero	Control	Definición
No	Control 1	

En definitiva, el objetivo de esta etapa es presentar los controles más efectivos para mitigar los riesgos identificados.

2.3.2 Creación Modelo de auditoria

La creación de un modelo para la ejecución de auditorías es un paso fundamental en el ámbito de la gestión de riesgos y la seguridad de la información. Este proceso se erige como un pilar esencial para garantizar la integridad, la confidencialidad y la disponibilidad de los activos digitales de una organización. Al desarrollar un modelo de auditoría sólido, se establece un marco de trabajo estructurado y eficiente que permite evaluar de manera sistemática los sistemas, procesos y controles de seguridad. Este modelo proporciona una hoja de ruta que guía a los profesionales de auditoría y seguridad a través de los pasos necesarios para identificar y mitigar riesgos, asegurando así la protección de la información crítica y el cumplimiento de requisitos normativos y legales.

2.3.3 Construcción del modelo de auditoría de seguridad para sistemas industriales SCADA

Para desarrollar esta metodología de ejecución de auditoría basada en el Marco de Ciberseguridad del NIST (CSF), se tienen en cuenta varios enfoques y referencias. Estos incluyen elementos del ciclo de Deming y las directrices de la norma ISO 19011, que contribuyen al ciclo de vida de la auditoría. Estos componentes se agregan para mejorar la metodología y garantizar una gestión eficiente a lo largo de todo el proceso de auditoría, desde la planificación hasta la conclusión. Esto permite una mejora continua y sistemática en la seguridad de las infraestructuras SCADA.

En la fase de 'Planificar', para ello se definieron los objetivos y el alcance de la auditoría, guiados por las directrices del CSF del NIST y las necesidades específicas de seguridad en infraestructuras SCADA. Además, se identifican los riesgos potenciales y se desarrollan estrategias para mitigarlos, se definen los KPI (Indicadores Clave de Rendimiento) de seguridad y establecen las políticas de seguridad y se planifican los recursos necesarios. Se diseña el plan de auditoría, incluyendo el alcance, la metodología y el cronograma. Este enfoque resalta la importancia de una planificación meticulosa, siendo el primer paso concluyente en cualquier proceso de mejora continua.

Durante la fase de 'Hacer', se ejecutan las auditorías según los procedimientos definidos en el plan, recopilando datos y evidencias esenciales para una evaluación exhaustiva. Esto con base en los procesos y controles de seguridad planificados. Al mismo tiempo, se ejecuta el plan de auditoría, realizando evaluaciones de vulnerabilidades, pruebas de penetración, revisión de configuración, etc. Se recopilaron datos sobre el rendimiento de los controles de seguridad, se documentaron todas las actividades y hallazgos y se implementaron medidas de seguridad inmediatas para abordar vulnerabilidades críticas identificadas durante la auditoría.

La etapa de 'Verificar' desempeña un papel concluyente al evaluar los resultados de la auditoría con base en los criterios de riesgo y los controles del CSF del NIST, garantizando el cumplimiento de los estándares de seguridad requeridos. Se analizan los datos recopilados

durante la fase de "Hacer". Se realizan análisis de causa raíz para los problemas de seguridad encontrados.

En resumen, la combinación del CSF del NIST y el ciclo de Deming proporciona a la metodología de auditoría un enfoque integral y sistemático. Este modelo no solo busca evaluar y proteger las infraestructuras SCADA, sino también impulsar su evolución constante. Al integrar la mejora continua en el proceso de auditoría

2.4 Fase 4: Validar el modelo de seguridad para la ejecución de una auditoria sobre los sistemas industriales, considerando los riesgos y controles propuestos

Para la realización de un caso de estudio con el objetivo de validar la metodología de ejecución de auditoría de seguridad para infraestructura SCADA. Este método tenía como objetivo poner a prueba la eficacia de la metodología y su capacidad para detectar y abordar riesgos de seguridad en entornos críticos. Todas las etapas de la metodología, desde la planificación hasta la implementación de acciones correctivas, y finalmente la comunicación de los resultados, se evaluaron en el caso de estudio, que se diseñó como un escenario controlado.

2.4.1 Crear un caso de estudio

El caso de estudio se diseñó para simular un entorno típico de infraestructura SCADA, como podría ser una central eléctrica o una planta de tratamiento de agua. En estos entornos, la seguridad y la disponibilidad de los sistemas son de vital importancia debido a las implicaciones directas en la operación y la seguridad pública. Durante la auditoría simulada, se realizaron análisis exhaustivos de múltiples aspectos críticos. Esto incluyó la evaluación de los controles de seguridad implementados, la revisión de las políticas de acceso para garantizar que fueran adecuadas y seguras, así como la revisión de las configuraciones del sistema para identificar posibles vulnerabilidades. Además, se examinaron los procedimientos y la capacidad de respuesta ante riesgos para asegurar que estuvieran bien definidos y fueran efectivos en la mitigación de riesgos y la restauración rápida de los servicios en caso de interrupciones o ataques. Para el caso de estudio se definieron los siguientes enunciados:

1. Objetivo del caso de estudio
2. Introducción
3. Alcance
4. Contexto de la empresa
5. Infraestructura TIC
6. Problemática
7. Expectativas

Caso de estudio:

1. Objetivo: El objetivo de este caso de estudio fue evaluar la efectividad del modelo propuesto para la realización de auditorías de seguridad en sistemas industriales SCADA, haciendo uso de buenas prácticas internacionales.
2. Introducción: se debe describir brevemente el propósito del caso de estudio, resaltando la importancia de la seguridad en los sistemas industriales SCADA y la necesidad de establecer un enfoque metodológico basado en buenas prácticas internacionales.
3. Alcance: Es importante definir como la delimitación de los sistemas industriales SCADA y las áreas específicas que serán evaluadas durante la auditoría de seguridad. Esto incluye los componentes y protocolos utilizados, así como las redes y dispositivos involucrados.
4. Contexto de la empresa: es importante proporcionar una descripción de la empresa en la que se lleva a cabo el caso de estudio. Incluye detalles sobre su industria, el tipo de sistema industrial SCADA utilizado y el papel de este sistema en sus operaciones.
5. Infraestructura TIC: se proporcionó una descripción detallada de la infraestructura tecnológica de la empresa, incluyendo la arquitectura de red, los servidores, los equipos terminales, los sistemas operativos y cualquier otro componente relevante.
6. Problemática: En este apartado se explicó como los desafíos o problemas relacionados con la seguridad en los sistemas industriales SCADA que la empresa enfrenta actualmente. donde se mencionó posibles brechas de seguridad, amenazas comunes o vulnerabilidades identificadas.
7. Expectativas: Se definen las expectativas que se tienen al llevar a cabo la auditoría de seguridad utilizando el modelo propuesto. Esto podría incluir la identificación de vulnerabilidades, recomendaciones de mejora, cumplimiento de estándares internacionales, entre otros.

2.4.2 Validar el modelo de auditoría de seguridad para entornos industriales SCADA ejecutándolo en el caso de estudio

La validación del modelo de auditoría se llevó a cabo de manera exhaustiva, utilizando un caso de estudio propuesto y hojas de cálculo en Excel para verificar cada paso. Este enfoque permitió una evaluación cuantitativa y detallada, asegurando la solidez y coherencia del modelo en diferentes escenarios. Las planillas de Excel no solo registraron datos, sino que también facilitaron el análisis comparativo entre los resultados esperados y los obtenidos, identificando posibles brechas o áreas de mejora. La validación práctica, alineada con nuestro enfoque metodológico, no solo respalda la efectividad del modelo, sino que también ofrece oportunidades para ajustes refinados basados en la experiencia práctica, maximizando así su utilidad en situaciones reales de auditoría.

3. Resultados

Conforme a la metodología delineada en el capítulo anterior, se procede a la exposición de los resultados derivados de cada una de las fases del proceso. Este enfoque metodológico estructurado ha guiado nuestras acciones, permitiendo una evaluación integral y detallada de los datos recopilados en cada etapa. La presentación de resultados constituye un paso crucial para compartir los hallazgos y conclusiones alcanzadas a lo largo del estudio.

Cada fase se analizará de manera individual, desglosando los datos y las observaciones pertinentes. Esta presentación detallada no solo brinda transparencia en el proceso de investigación, sino que también sirve como base para la discusión y la interpretación de los resultados obtenidos. La coherencia con la metodología establecida garantiza la fiabilidad y relevancia de los resultados, respaldando así la validez de las conclusiones derivadas de este estudio.

3.1 Fase 1: Generar un mapa de riesgos en los sistemas industriales, identificando amenazas y vulnerabilidades

3.1.1 Identificación de los activos mínimos de un sistema SCADA

Durante el proceso de investigación, al llevar a cabo consultas exhaustivas tanto en las páginas web de productores especializados como en la plataforma de Google Académico, se obtuvo información crucial que arrojó luz sobre los activos mínimos esenciales en un sistema industrial SCADA. Esta investigación meticulosa y enriquecedora ha permitido identificar con precisión los componentes fundamentales que conforman la infraestructura de un sistema SCADA, cuya robustez y continuidad operativa son vitales para asegurar el funcionamiento eficiente y seguro de procesos industriales como se muestra en la (tabla 19) donde se menciona los ítems de las fuentes de consulta.

Tabla 20.

Referencias de consulta activos SCADA

Item	Referencia web o tesis	Autor
1	Introducción a SCADA	Hugo Pérez - UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
2	Introducción a SCADA	Asignatura: Interfaz Hombre Máquina Profesores: Carlos de Castro Lozano Cristóbal Romero Morales
3	Metodología propuesta para la auditoría de seguridad cibernética en un sistema SCADA	Ricardo Alonso Torres Valero Fabian Andrés Medina Becerra Miguel Ángel Mendoza Moreno

4	https://www.incibe-cert.es/blog/inventario-activos-y-gestion-seguridad-sci	Incibe

Nota. La tabla muestra referencias relacionadas con SCADA.

Estos activos mínimos esenciales constituyen la columna vertebral de un sistema SCADA confiable y efectivo, y su identificación se basa en una investigación rigurosa que combina fuentes de información de alta calidad para garantizar la integridad y la continuidad operativa de procesos industriales críticos. La (tabla 20) recoge los activos críticos mínimos del funcionamiento de un sistema SCADA.

Tabla 21.

Activos mínimos de un sistema industrial SCADA

No	ACTIVO	TIPO
1	RTU	Físico
2	PLC	Físico
3	Servidor	Físico
4	HMI	Físico
5	Software SCADA	Lógico
6	Base de datos	Lógico
7	Personal interno	Personal
8	Red	Comunicación

Nota. La tabla muestra tipos de activos.

La tabla anterior muestra los activos son esenciales para el funcionamiento de un sistema SCADA y se pueden clasificar en tres categorías principales:

- Activos físicos: Estos son componentes tangibles como RTU, PLC, servidores, HMI y redes. Son responsables de la adquisición de datos, el control de procesos y la comunicación entre los diferentes componentes del sistema.
- Activos lógicos: Estos son componentes intangibles como el software SCADA y las bases de datos. Son responsables del procesamiento de datos, la supervisión del sistema, la generación de informes y la toma de decisiones.
- Activos de personal: Estos son las personas que operan, mantienen y administran el sistema SCADA. Su conocimiento, habilidades y experiencia son cruciales para el correcto funcionamiento del sistema.

Por lo tanto, la tabla proporciona una base sólida para la evaluación de riesgos de un sistema SCADA. Al comprender los activos involucrados y sus funciones, se puede identificar y priorizar los riesgos potenciales que podrían afectar la seguridad y la confiabilidad del sistema.

Por tanto, clasificar los activos en estas categorías ayuda a priorizar la protección y gestión de cada tipo de activo, identificando las amenazas y vulnerabilidades específicas que puedan afectarlos y aplicando medidas de seguridad adecuadas. La seguridad de un sistema SCADA depende de la protección integral de estos diversos activos.

3.1.2 Identificación de amenazas y vulnerabilidades

Durante el proceso de investigación, se llevó a cabo un análisis exhaustivo de las amenazas y vulnerabilidades que afectan a sistemas SCADA, utilizando diversas fuentes de información confiables. Estas fuentes proporcionaron una visión completa de los riesgos que pueden comprometer la seguridad de las infraestructuras SCADA.

la recopilación de datos de múltiples fuentes confiables, incluyendo páginas web especializadas, bases de datos de vulnerabilidades e informes de seguridad, ha permitido obtener una visión detallada y actualizada de las amenazas y vulnerabilidades que deben abordarse en la auditoría de seguridad de sistemas SCADA. La lista de sitios de consulta se presenta en la tabla 21:

Tabla 22.

Sitios de consulta de amenazas y vulnerabilidades

Item	Pagina web	Sigla
1	https://www.nist.gov/search?s=scada+vulnerabilities&index=all-meta-engine	NIST
2	https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=scada	CVE
3	https://www.cisecurity.org/search?page=1&s=scada+vulnerabilities	CIS
4	https://scadahacker.com/	

Nota. La tabla muestra las webs de amenazas y vulnerabilidades.

De las diversas fuentes consultadas, se logró identificar y documentar un conjunto de siete (7) problemáticas de seguridad críticas (como se detalla en la Tabla 22) que tienen el potencial de generar impactos negativos significativos en los sistemas SCADA. Estas amenazas y vulnerabilidades presentan una variedad de riesgos que abarcan desde interrupciones en la operación normal hasta posibles daños materiales y riesgos para la seguridad pública. Es esencial comprender y abordar estas problemáticas para garantizar la disponibilidad, integridad y confiabilidad de los componentes y activos críticos de infraestructuras SCADA.

Tabla 23.

Identificación de amenazas y vulnerabilidades

Amenaza	Vulnerabilidad
Phishing	Falta de concientización del personal, falta de filtros de correo electrónico, falta de segmentación en la red.
Malware	Falta de actualizaciones y parches, falta de controles de acceso y autenticación, configuraciones de seguridad débiles, vulnerabilidades en software y hardware, falta de políticas y procedimientos de seguridad, fallos en la supervisión y detección de anomalías.
DoS	Falta de redundancia, configuraciones de seguridad débiles, insuficientes controles de autenticación y autorización, vulnerabilidades en el software y hardware, falta de procedimientos de respuesta a riesgos, falta de políticas de seguridad y entrenamiento del personal.
Acceso no autorizado	software desactualizado, Puertos no protegidos, contraseña por defecto, falta de monitoreo.
Fallos humanos	Falta de concienciación y entrenamiento del personal, errores en la configuración y operación de sistemas, falta de supervisión y detección de anomalías, falta de políticas de seguridad y procedimientos de seguridad.
Buffer overflow	Falta de validación de entrada, Desbordamiento de búfer, Error en la gestión de memoria
Inyección de código	Fallos de validación, falta de medidas de seguridad en la programación, falta de validación de entrada de datos

Nota. La tabla muestra las problemáticas de seguridad críticas.

Estas problemáticas de seguridad requieren una atención cuidadosa y medidas de mitigación adecuadas para proteger los sistemas SCADA contra amenazas y vulnerabilidades potenciales. La identificación de estas problemáticas es un primer paso fundamental en el proceso de auditoría de seguridad, ya que permite enfocar los esfuerzos en las áreas críticas que requieren una evaluación minuciosa y medidas de corrección efectivas.

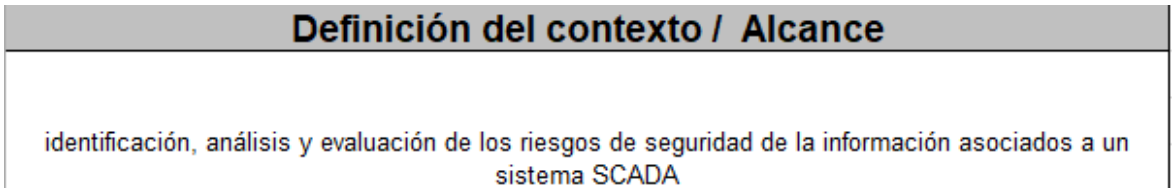
3.1.3 Elaboración de mapa de riesgos

El análisis de riesgos conforme a los principios de la norma ISO 27005 mediante la utilización de la herramienta de Microsoft Excel. Este proceso se ejecutó siguiendo los siguientes pasos que habían sido previamente definidos y establecidos:

1. Para la generación del mapa de riesgo en el marco de este proyecto de grado, se definió un contexto sólido basado en la identificación, análisis y evaluación de una serie de criterios clave. Estos criterios han sido cuidadosamente seleccionados y están estrechamente alineados con los objetivos del proyecto, con el propósito de garantizar una gestión de riesgos efectiva y coherente.

Tabla 24.

Concepto de mapa de riesgo



2. La identificación de los activos se basa en una lista mínima de activos previamente consolidada, la cual se detalla en el numeral 3.1.1 de la actividad 1.

Tabla 25.

Activos mínimos del sistema SCADA

Categoría	Activo/Recurso	Descripción	Detalles adicionales
Físico	PLC (Controlador Lógico Programable)	Un controlador basado en microprocesador utilizado para automatizar procesos industriales	Modelo: Siemens S7-300
Físico	RTU (Unidad Terminal Remota)	Un dispositivo que recopila y transmite datos de sensores y dispositivos de campo	Cantidad: 10
Físico	Servidor	Una computadora que almacena y procesa datos para el sistema SCADA	Sistema operativo: Windows Server 2019
Físico	HMI (Interfaz Hombre-Máquina)	Un dispositivo que permite a los operadores interactuar con el sistema SCADA	Tipo: Panel táctil de 15"
Lógico	Software SCADA	El software que administra y controla el sistema SCADA	Nombre: Wonderware System Platform
Lógico	Base de datos	Un repositorio para almacenar y administrar datos del sistema SCADA	Tipo: Base de datos relacional MySQL
Personal	Personal interno	Personas responsables de operar, mantener y administrar el sistema SCADA	Operaciones: Monitorear y controlar el sistema SCADA, responder a alarmas
Comunicación	Red de comunicación	La red que conecta los componentes del sistema SCADA	Topología: Estrella

Nota. La tabla muestra lista mínima de activos.

3. Para evaluar el grado de clasificación de la información, se recurre a las escalas de clasificación específicas establecidas por una entidad del sector, como se mencionó previamente en el enfoque metodológico, que comprenden categorías como confidencial, privada o pública, y se detallan a continuación.

Nivel de clasificación Confidencial: se advierte sobre la confidencialidad de la información financiera, técnica y cualquier otro tipo de datos utilizados por empleados, terceros o aprendices dentro de la organización. Esta información no debe ser accesible para personas externas sin una autorización expresa del presidente de la empresa, el Gerente General o el director del área responsable de su generación y uso. La divulgación, uso o modificación no autorizada de esta información podría tener consecuencias adversas significativas en los acuerdos, sistemas y procesos de la compañía.

Nivel de clasificación Privada: Se incluye la información financiera, técnica y cualquier otro tipo de datos utilizados por empleados, terceros o aprendices dentro de la organización, los cuales no deben ser accesibles para individuos externos sin la debida autorización del responsable de la unidad o proyecto encargado de la creación y uso de dicha información. La divulgación, uso o modificación no autorizada de esta información podría tener un impacto significativo en terceros o en los sistemas y procesos de la compañía.

Nivel de clasificación Pública: Se ha incorporado información de carácter general utilizada por empleados, terceros o aprendices dentro de la organización, la cual no debe ser divulgada a personas externas sin la autorización adecuada del responsable de la información. En caso de que esta información sea revelada, utilizada o alterada por individuos no autorizados, no tendría un impacto significativo en los clientes, sistemas o procesos de la empresa.

A continuación, se describe el proceso de valoración del nivel de clasificación de los activos (tabla 23):

Se han establecido 4 posibles factores de impacto que un activo puede experimentar si es modificado, eliminado o dañado.

Cada uno de estos factores de afectación debe ser calificado en una escala que abarca desde 1 hasta 4, donde 1 representa el nivel mínimo de afectación y 4 el nivel máximo de afectación.

En el caso de que un activo presente el valor más alto en todos los factores de afectación, su puntuación total será de 20.

La valoración de los niveles de clasificación se realiza en función de los puntajes totales, siguiendo estos criterios:

a. Clasificación Pública: Si el valor total de los factores de afectación se encuentra por debajo de 8, lo que indica que no representa un riesgo significativo.

b. Clasificación Privada: Si el valor total de los factores de afectación está en el rango de 8 a 15, lo que denota un nivel medio de riesgo.

c. Clasificación Confidencial: Si el valor total de los factores de afectación supera los 15, lo que señala un riesgo elevado.

El sistema realiza el cálculo del valor total y la clasificación asignada a cada activo de información. Esto marca el comienzo de la siguiente etapa en la metodología de gestión de riesgos.

Tabla 26.

Clasificación de los activos vs los impactos industriales.

Activo	Afectación sobre los planes de negocio (finanzas).	Tipo de destinatario	Afecta legalmente a la empresa	Afecta las ventas o una ventaja competitiva.	Tiene afectación sobre la seguridad	Nivel de criticidad	
PLC	4	4	1	4	4	17	confidencial
RTU	4	4	1	4	4	17	confidencial
SERVIDOR MTU, HISTORIAL	4	4	1	4	4	17	confidencial
EQUIPAMENTO PANTALLA HMI	4	4	2	4	4	18	confidencial
SOFTWARE SCADA	4	4	4	4	4	20	confidencial
DATOS (BASE DE DATOS)	4	4	4	4	4	20	confidencial
PERSONAL INTERNO	3	3	4	2	4	16	confidencial
RED DE COMUNICACIONES	4	4	4	4	4	20	confidencial

Nota. La tabla muestra la clasificación asignada a cada activo de información. *Fuente: tomado de* **[60]**.

Las tres categorías de activos (pública, privada y confidencial) se utilizaron para clasificarlos. Las empresas deben tener en cuenta estas categorías al tomar decisiones. En el estudio de auditoría de infraestructuras críticas, estas categorías son esenciales para la gestión de controles. Se puede clasificar la información comercial en una de estas tres categorías según su importancia. A pesar de que los activos críticos son accesibles dentro de la organización, deben protegerse. Como resultado, la clasificación indica que más del 90 % de los activos se consideran finalmente confidenciales. Cada uno de estos activos contiene información específica sobre las organizaciones a las que se prestan servicios según el alcance definido. Es fundamental asegurarse de que la información contenida en los activos críticos no esté expuesta a cambios o esté disponible para personas externas. Este método se utiliza para garantizar la equidad en los acuerdos porque la información contenida en estos activos puede utilizarse para explotar vulnerabilidades, lo que podría resultar en daños graves o pérdidas significativas para la empresa.

La existencia de una vulnerabilidad por sí sola no genera perjuicio, dado que se necesita una amenaza en curso para que sea aprovechada. Una vulnerabilidad que no representa un riesgo inmediato puede no necesitar la aplicación de un control, pero debe ser identificada y monitoreada en caso de futuros cambios [40].

4. Se examinaron los controles que ya estaban en el sistema durante esta etapa centrada en la identificación de controles. Los resultados mostraron que la mayoría de los controles aplicados seguían ajustes predeterminados por defecto, mientras que otros estaban incompletos o completamente desconocidos. Es importante destacar que estos hallazgos se realizaron en un entorno académico, donde el sistema no estaba equipado con controles de seguridad fuertes o altamente personalizados. El objetivo principal era enseñar los conceptos de seguridad de la información en lugar de priorizar la implementación de medidas de seguridad avanzadas.
5.

- **0%**: No se han implementado controles.
- **25%**: Algunos controles están implementados, pero no funcionan adecuadamente o son limitados, lo que implica que no cubren completamente el riesgo identificado.
- **50%**: Todos los controles propuestos están implementados, pero aún no se ha validado su efectividad.
- **75%**: Todos los controles están implementados y se verifica su efectividad, pero no se realiza un monitoreo continuo ni se elaboran planes de mejora continua.
- **100%**: Todos los controles están implementados, se mide su efectividad mediante líneas base periódicas y auditorías, y se generan planes de acción para su mantenimiento y mejora continua.

Tabla 27.

Vulnerabilidades vs impacto

Activos	**Vulnerabilidades**	**Controles actuales implementados en el activo.**	**Clasificación del activo**	**Efectividad de los controles = Eficiencia + Eficacia**
PLC	falta de políticas y procedimientos de seguridad, sin políticas de parchado, falta de control de acceso, errores en la configuración y	N/A	Confidencial	0%

	operación de sistemas			
RTU	falta de políticas y procedimientos de seguridad, sin políticas de parchado, falta de control de acceso, errores en la configuración y operación de sistemas	N/A	Confidencial	0%
SERVIDOR MTU, HISTORIAL	falta de políticas y procedimientos de seguridad, sin políticas de parchado, falta de control de acceso, errores en la configuración y operación de sistemas	N/A	Confidencial	0%
EQUIPAMENTO PANTALLA HMI	falta de políticas y procedimientos de seguridad, sin políticas de parchado, falta de control de acceso, vulnerabilidades en el software, falta redundancia, falta de medidas de seguridad en la programación, errores en la configuración y operación de sistemas	N/A	Confidencial	0%
SOFTWARE SCADA	Falta de validación de entrada, Desbordamiento de búfer, Error en la gestión de memoria	N/A	Confidencial	0%

DATOS (BASE DE DATOS)	Puertos no protegidos, contraseña por defecto, falta de monitoreo, errores en la configuración y operación de sistemas	N/A	Confidencial	0%
PERSONAL INTERNO	Falta de concienciación y entrenamiento del personal	N/A	N/A	0%
RED DE COMUNICACIONES	falta de segmentación en la red, falta de políticas y procedimientos de seguridad, falta de monitoreo, Puertos no protegidos	N/A	Confidencial	0%

Nota. La tabla muestra una discriminación de vulnerabilidades vs impactos de los diferentes activos.

La tabla proporciona una visión general de las vulnerabilidades identificadas en los activos, la efectividad de los controles actuales y el impacto potencial de la explotación de las vulnerabilidades.

6. En este paso, se procedió a incorporar lo previamente recolectado durante la fase de identificación de amenazas y vulnerabilidades, como se documentó en la tabla 22. Esta información recopilada es importante, dado que proporciona una base sólida para el proceso en curso y permitirá una evaluación de los riesgos de seguridad de la información. El conocimiento de las amenazas identificadas es esencial para comprender y mitigar adecuadamente los riesgos asociados a la infraestructura critica.

Tabla 28.

Amenazas y factor de riesgo

Listado amenazas	Factor de riesgos
Phishing	**AMENAZAS TIC**
Malware	**AMENAZAS TIC**
DoS	**AMENAZAS TIC**
Buffer overflow	**AMENAZAS TIC**
Inyección de código	**AMENAZAS TIC**
Acceso no autorizado	**AMENAZAS ESTRATÉGICAS Y ADMINISTRATIVAS**
Fallos humanos	**AMENAZAS HUMANAS/SOCIALES**

Nota. La tabla muestra una evaluación de los riesgos de seguridad de la información.

En la evaluación de los controles existentes, se ha constatado que actualmente se encuentra implementado un 0%. Este dato refleja la ausencia de implementación de cualquier control de seguridad. Es fundamental destacar que este escenario se enmarca en un contexto puramente académico, lo que acentúa la importancia tanto de proponer controles de ciberseguridad como de desarrollar un modelo de auditoría adaptado a las necesidades de seguridad de los activos críticos de la organización. Este enfoque académico permite analizar y diseñar estrategias efectivas para fortalecer la seguridad de los activos críticos, en línea con las mejores prácticas de ciberseguridad.

7. En la tabla siguiente, se llevó a cabo una enumeración de las amenazas en comparación con los activos, con el objetivo de iniciar un proceso de reconocimiento integral. Este proceso es fundamental para crear un análisis cruzado de escenarios, donde se establece una conexión entre la probabilidad de que una amenaza específica pueda incidir en un activo concreto. Al realizar este cruce de información, se obtiene una visión más clara de cómo las amenazas potenciales pueden afectar a los activos de la organización.

Tabla 29.

Escenario (Activos vs Amenazas)

AMENAZAS / **ACTIVOS**	PLC	RTU	SERVIDOR MTU, HISTORIAL	EQUIPAMENTO PANTALLA	SOFTWARE SCADA	DATOS (BASE DE DATOS)	PERSONAL INTERNO	RED DE COMUNICACIONES
Phishing	x	x	**x**	**x**	**x**	**x**	**x**	**x**
Malware	x	x	**x**	**x**	**x**	**x**	**x**	**x**
DoS	x	x	**x**	**x**	**x**	**x**	**x**	**x**
Buffer overflow	x	x	**x**	**x**	**x**	**x**	**x**	**x**
Inyección de código	x	x	**x**	**x**	**x**	**x**	**x**	**x**
Acceso no autorizado	x	x	**x**	**x**	**x**	**x**	**x**	**x**
Fallos humanos	x	x	**x**	**x**	**x**	**x**	**x**	**x**

Nota. La tabla muestra una enumeración de las amenazas en comparación con los activos.

8. Después de identificar posibles situaciones, se inicia la etapa de evaluación utilizando las tablas de impacto establecidas en la metodología. En este punto, se pone de manifiesto la situación actual en términos de la eficacia de los controles existentes y los efectos potenciales en caso de que un activo resulte comprometido.
9. El cruce de escenarios ha arrojado un total de 56 riesgos, los cuales, una vez identificados, se someten a las tablas correspondientes para determinar tanto su probabilidad como su impacto.
10. El proceso de evaluación de escenarios de riesgo implica la selección de qué tan probable es que un evento se materialice, con el propósito de cuantificar su impacto. Para realizar esta evaluación, se hacen uso de las tablas predefinidas de probabilidad e impacto, y se toman en cuenta tanto la efectividad de los controles existentes como la clasificación de la información.

Tabla 30.

Impacto en la información pilar disponibilidad

Escenario de riesgos	Probabilidad	Impacto Operación	Riesgo P*Impacto Cliente Mercado	Clasificación del activo	Controles Asociados
Posibilidad que la amenaza: Phishing, afecte el activo: PLC	Posible	3	Mayor	4	12
Posibilidad que la amenaza: Phishing, afecte el activo: RTU	Posible	3	Mayor	4	12
Posibilidad que la amenaza: Phishing, afecte el activo: SERVIDOR MTU, HISTORIAL	Posible	3	Mayor	4	12
Posibilidad que la amenaza: Phishing, afecte el activo: EQUIPAMIENTO PANTALLA HMI	Posible	3	Intermedio	3	9
Posibilidad que la amenaza: Phishing, afecte el activo: SOFTWARE SCADA	Posible	3	Mayor	4	12
Posibilidad que la amenaza: Phishing, afecte el activo: DATOS (BASE DE DATOS)	Probable	4	Mayor	4	16

Nota. La tabla muestra la evaluación de escenarios de riesgo.

Los resultados de cada escenario se tabulan en la matriz 5*5 de criticidad que refleja una mirada holística del riesgo en la organización. Ver anexo 1 mapa de Riesgos.

11. Como conclusión, la distribución porcentual resultante (según se muestra en la Tabla 31 y la Figura 14) señala la necesidad de abordar la totalidad de los riesgos, con un 23.64% de estos clasificados como naranjas y el 76.36% como riesgos rojos. Es esencial destacar que la ineficacia de los controles, tal como se mencionó previamente en este ejemplo de carácter educativo, se debe a la ausencia de controles o a la presencia de controles predeterminados que sirven como incentivos para posibles atacantes, debido a su vulnerabilidad. Por tanto, resulta imperativo trabajar en la mejora de la efectividad y en la implementación de nuevos controles. Esta situación se origina en el contexto de la evolución tecnológica, especialmente en el ámbito de Internet de las cosas (IoTT).

Tabla 31.

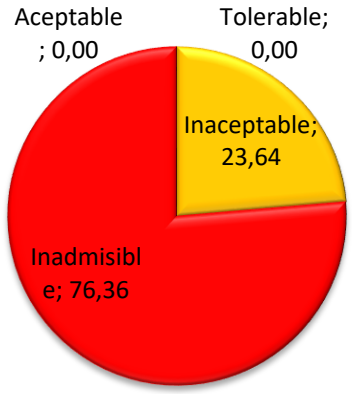
Matriz de riesgo

Distribución Porcentual		
ZONA	**%**	**Total Riesgos**
Aceptable	**0,00**	**0**
Tolerable	**0,00**	**0**
Inaceptable	**23,64**	**13**
Inadmisible	**76,36**	**42**

Nota. La tabla muestra los riesgos críticos.

Figura 14.

Distribución porcentual de riesgos



Nota. La figura muestra los porcentajes de riesgos prevaleciendo el inadmisible.

12. En la Tabla 30 del Plan de Tratamiento de Riesgos, se logró identificar los riesgos críticos, los cuales abarcan la totalidad de los riesgos que serán sometidos a control en la etapa 3. En esta fase, se propondrán los controles apropiados para un sistema industrial SCADA con el propósito de mitigar dichos riesgos críticos. La implementación de estos controles marca el inicio de la metodología de auditoría, que se enfocará en verificar el cumplimiento efectivo de estos controles. El

objetivo de este enfoque es cerrar las brechas que puedan surgir durante la definición de los ciclos de gestión de riesgos, asegurando una administración de riesgos adecuada y eficiente.

Tabla 32.

Riesgos Inaceptable, Inadmisible

RIESGOS ALTOS Considerando los controles actuales	
(1) -Posibilidad que la amenaza: Phishing, afecte el activo: PLC	(15) -Posibilidad que la amenaza: Malware, afecte el activo: PERSONAL INTERNO
(2) -Posibilidad que la amenaza: Phishing, afecte el activo: RTU	(16) -Posibilidad que la amenaza: Malware, afecte el activo: RED DE COMUNICACIONES
(3) -Posibilidad que la amenaza: Phishing, afecte el activo: SERVIDOR MTU, HISTORIAL	(17) -Posibilidad que la amenaza: DoS, afecte el activo: PLC
(4) -Posibilidad que la amenaza: Phishing, afecte el activo: EQUIPAMENTO PANTALLA HMI	(18) -Posibilidad que la amenaza: DoS, afecte el activo: RTU
(5) -Posibilidad que la amenaza: Phishing, afecte el activo: SOFTWARE SCADA	(19) -Posibilidad que la amenaza: DoS, afecte el activo: SERVIDOR MTU, HISTORIAL
(6) -Posibilidad que la amenaza: Phishing, afecte el activo: DATOS (BASE DE DATOS)	(20) -Posibilidad que la amenaza: DoS, afecte el activo: EQUIPAMENTO PANTALLA HMI
(7) -Posibilidad que la amenaza: Phishing, afecte el activo: PERSONAL INTERNO	(21) -Posibilidad que la amenaza: DoS, afecte el activo: SOFTWARE SCADA
(8) -Posibilidad que la amenaza: Phishing, afecte el activo: RED DE COMUNICACIONES	(22) -Posibilidad que la amenaza: DoS, afecte el activo: DATOS (BASE DE DATOS)
(9) -Posibilidad que la amenaza: Malware, afecte el activo: PLC	(23) -Posibilidad que la amenaza: DoS, afecte el activo: PERSONAL INTERNO
(10) -Posibilidad que la amenaza: Malware, afecte el activo: RTU	(24) -Posibilidad que la amenaza: DoS, afecte el activo: RED DE COMUNICACIONES
(11) -Posibilidad que la amenaza: Malware, afecte el activo: SERVIDOR MTU, HISTORIAL	(25) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: PLC
(12) -Posibilidad que la amenaza: Malware, afecte el activo: EQUIPAMENTO PANTALLA HMI	(26) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: RTU
(13) -Posibilidad que la amenaza: Malware, afecte el activo: SOFTWARE SCADA	(27) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: SERVIDOR MTU, HISTORIAL
(14) -Posibilidad que la amenaza: Malware, afecte el activo: DATOS (BASE DE DATOS)	(28) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: EQUIPAMENTO PANTALLA HMI

Nota. La tabla muestra los controles apropiados para un sistema industrial SCADA.

La tabla anterior de riesgos muestra una lista de 28 escenarios de riesgo, cada uno con una amenaza específica que podría afectar a un activo de seguridad en sistemas industriales. La tabla también incluye la probabilidad de ocurrencia y el impacto potencial de cada riesgo, clasificándolos como "Inaceptable", "Inadmisible", "Aceptable" o "Tolerable". A continuación, se presenta un análisis de la información que proporciona la tabla:

Distribución de Riesgos por Categoría:

- Inaceptable (23%): Esta categoría representa la mayor cantidad de riesgos, lo que indica que la seguridad en sistemas industriales enfrenta un nivel significativo de riesgos que podrían tener un impacto grave en sus operaciones.
- Inadmisible (18%): Esta categoría también representa una cantidad considerable de riesgos, lo que reitera la necesidad de que se tomen medidas urgentes para mitigar estos riesgos.
- Aceptable (20%): Esta categoría representa una cantidad moderada de riesgos que se están gestionando de manera adecuada.
- Tolerable (29%): Esta categoría representa la menor cantidad de riesgos, lo que indica que se tiene un buen control sobre estos riesgos.

Riesgos Inaceptables e Inadmisibles:

La tabla destaca 28 riesgos que han sido clasificados como "Inaceptable" o "Inadmisible". Estos riesgos representan una seria amenaza de seguridad en sistemas industriales y requieren una atención inmediata. Algunos ejemplos de estos riesgos incluyen:

- Ataques de phishing que comprometen activos críticos como PLC, RTU, servidores y bases de datos.
- Infecciones de malware que afectan la operación de PLC, RTU, software SCADA y equipos HMI.
- Ataques de denegación de servicio (DoS) que afectan la disponibilidad de PLC, RTU, servidores y redes de comunicación.
- Exposición de datos confidenciales debido a ataques de phishing, malware o errores humanos.

Impacto Potencial de los Riesgos:

La tabla también proporciona información sobre el impacto potencial de cada riesgo. El impacto está clasificado como "Mayor", "Intermedio" o "Bajo". Es importante considerar tanto la probabilidad como el impacto de cada riesgo para determinar su prioridad.

Amenazas Identificadas:

La tabla identifica las siguientes amenazas principales:

- Phishing: Esta amenaza implica ataques de suplantación de identidad que buscan obtener información confidencial o acceso no autorizado a sistemas.
- Malware: Esta amenaza implica software malicioso que puede dañar sistemas, robar datos o interrumpir operaciones.

- DoS: Esta amenaza implica ataques que buscan sobrecargar sistemas o redes para hacerlos inaccesibles.

- Buffer overflow: Esta amenaza implica vulnerabilidades de software que pueden permitir a los atacantes ejecutar código arbitrario en un sistema.

Activos Afectados:

La tabla también muestra los activos que podrían verse afectados por cada riesgo. Los activos más comunes incluyen:

- PLC: Controladores lógicos programables utilizados para automatizar procesos industriales.

- RTU: Unidades terminales remotas utilizadas para recopilar y transmitir datos de campo.

- Servidores: Sistemas informáticos que almacenan y procesan datos.

- Software SCADA: Sistemas de control y supervisión de SCADA utilizados para gestionar infraestructuras críticas.

- Bases de datos: Repositorios de datos electrónicos que almacenan información confidencial.

- Equipos HMI: Interfaces hombre-máquina utilizados para interactuar con sistemas de control.

- Redes de comunicación: Infraestructura que permite la comunicación entre sistemas.

- Personal interno: Empleados de la organización que pueden ser víctimas de ataques de ingeniería social o errores humanos.

Recomendaciones:

En base al análisis de la tabla, se considera tener en cuenta las siguientes acciones:

- Priorizar la mitigación de riesgos Inaceptables e Inadmisibles: se debe tomar medidas urgentes para mitigar los 28 riesgos que han sido clasificados como "Inaceptable" o "Inadmisible". Esto puede implicar implementar controles técnicos, organizativos o de concienciación, o incluso eliminar los riesgos si es posible.

- Evaluar y tratar riesgos Aceptables y Tolerables: Si bien los riesgos "Aceptables" y "Tolerables" representan un menor nivel de amenaza, se debe continuar evaluándolos y tomando medidas para mitigarlos si es necesario.

- Implementar un programa de gestión de riesgos: La organización debe establecer un programa formal de gestión de riesgos que incluya procesos para identificar, evaluar, clasificar, tratar y comunicar los riesgos.

En conclusión, el mapa de riesgos creado para el sistema SCADA sin controles ha proporcionado una visión clara y detallada de las amenazas y vulnerabilidades que afectan al sistema en este análisis puramente académico. La creación y aplicación de controles efectivos se basará en esta información como base. Además, se desarrollará una técnica de auditoría que evaluará minuciosamente el cumplimiento de estos controles. Este procedimiento permitirá cerrar las brechas de seguridad y garantizar una gestión de riesgos sólida y adecuada en el sistema SCADA, lo que ayudará a fortalecer y proteger sus activos críticos. Los resultados de todos los riesgos de criticidad naranja y roja se encuentran refleja en el tratamiento de los riesgos. (Para más detalle ver Anexo 1).

3.2 Fase 2. Caracterizar normas, estándares o buenas prácticas que estén asociadas al proceso de auditoría en seguridad para ser aplicados a los entornos industriales

Siguiendo el plan establecido para alcanzar el objetivo, a continuación, se muestran los logros conseguidos. Caracterizar las normas para la creación de la estrategia para gestión de riesgos, considerando la norma COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF).

3.2.1 Caracterizar las normas para la creación de la estrategia para gestión de riesgos, considerando la norma COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF)

Para caracterizar las normas utilizadas en la elaboración de la metodología para auditar la seguridad de infraestructuras críticas y sistemas SCADA, considerando COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF), se pueden utilizar tres aspectos conceptuales para el análisis:

1. **Alcance y Objetivos**: Esta dimensión evalúa los objetivos y la cobertura de cada normativa en relación con la auditoría de seguridad. Por ejemplo, COBIT se centra en el gobierno y la gestión de TI, mientras que ISO/IEC 27001 está más orientada a la seguridad de la información en general.

2. **Estructura y Procesos**: Aquí se analiza la estructura y los procesos que cada normativa propone para la gestión y auditoría de la seguridad. ITIL, por ejemplo, ofrece un marco para la gestión de servicios de TI, mientras que el Marco de Ciberseguridad de NIST proporciona un conjunto de controles y prácticas para la ciberseguridad.

3. **Implementación y Medición**: Esta dimensión se enfoca en cómo se implementan las directrices y cómo se mide la efectividad de las prácticas propuestas por cada normativa. Por ejemplo, COSO incluye criterios de evaluación interna y COBIT define métricas para la medición del desempeño de los controles de TI.

A continuación, en la Tabla 32, se presenta una descripción general de estas normativas caracterizadas bajo estos tres aspectos conceptuales, proporcionando una visión integral de cómo cada una contribuye a la auditoría y gestión de la seguridad en infraestructuras críticas y sistemas SCADA.

Tabla 33.

Normas versus criterios

Norma/Criterios	Ventajas	Procesos	Enfoque
COSO	Se centra en el control interno y la gestión de riesgos, proporcionando una visión amplia y completa de la gestión de riesgos en una organización. Esto incluye la identificación, evaluación y respuesta a riesgos a nivel empresarial.	Ofrece un marco integral que abarca la evaluación de riesgos, la respuesta a riesgos y el control interno. Se centra en la evaluación de riesgos empresariales en general.	Se centra en la gestión de riesgos y control interno a nivel organizativo. Es adecuado para organizaciones que desean integrar la gestión de riesgos en sus procesos empresariales.
COBIT	Se enfoca en la gobernanza de TI y el control de procesos relacionados con la tecnología de la información. Esto lo hace adecuado para la gestión de riesgos de TI y ciberseguridad.	Proporciona un conjunto de procesos bien definidos y objetivos de control específicos que se relacionan con la gestión de riesgos de TI y la ciberseguridad.	Se centra en la gobernanza de TI y la alineación de TI con los objetivos del negocio, lo que lo hace particularmente útil para la gestión de riesgos tecnológicos.
ITIL	Se centra en la gestión de servicios de TI, lo que lo hace relevante para la gestión de riesgos de TI y la continuidad del negocio. Proporciona un enfoque estructurado para la gestión de servicios de TI.	Ofrece un conjunto de procesos y prácticas que abordan la gestión de riesgos y problemas, centrándose en la restauración de servicios y la minimización del impacto en el negocio.	Su enfoque principal es la gestión de servicios de TI, siendo adecuado para organizaciones que buscan establecer una estrategia para la gestión de riesgos de TI y la continuidad del negocio.
ISO/IEC 27001	es una norma de seguridad de la información ampliamente reconocida y adoptada a nivel mundial. Se centra en la seguridad de la información en general,	Proporciona procesos y controles específicos para la gestión de riesgos de seguridad de la información, incluyendo la identificación,	Se centra en la seguridad de la información y es especialmente adecuado para organizaciones que buscan una estrategia integral para la gestión

	lo que la hace relevante para la gestión de riesgos de seguridad.	evaluación y respuesta a riesgos de seguridad.	de riesgos de seguridad.
Marco de Ciberseguridad de NIST (CSF)	El CSF se desarrolló específicamente para la ciberseguridad y se centra en la identificación, protección, detección, respuesta y recuperación de riesgos de seguridad cibernética.	Ofrece un enfoque detallado para la gestión de riesgos de seguridad cibernética, con procesos bien definidos en cada una de sus cinco funciones.	Está diseñado para la ciberseguridad y es especialmente adecuado para organizaciones que buscan establecer una estrategia específica para la gestión de riesgos de seguridad cibernética

Nota: Esta tabla presenta la comparación de criterios vs normas.

La tabla presenta una comparación de seis marcos de referencia para la gestión de riesgos: COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF). Cada marco ofrece un enfoque y metodologías específicas para identificar, evaluar, tratar y comunicar riesgos en diferentes contextos.

En general, COSO ofrece una visión amplia y completa de la gestión de riesgos a nivel organizativo, mientras que COBIT se especializa en la gestión de riesgos de TI y la gobernanza de TI. ITIL es útil para la gestión de riesgos de TI y la continuidad del negocio, mientras que ISO/IEC 27001 proporciona una norma reconocida para la gestión de riesgos de seguridad de la información. El Marco de Ciberseguridad de NIST (CSF) está diseñado específicamente para la gestión de riesgos de seguridad cibernética. Por tanto, implementar un marco de referencia robusto para la gestión de riesgos puede ayudar a las organizaciones a identificar, evaluar, tratar y comunicar riesgos de manera efectiva, protegiendo sus activos y mejorando su resiliencia ante eventos adversos.

Por otra parte, después de describir cada una de las normas, se procede a enmarcar el objetivo general en tres criterios. Estos criterios buscan desarrollar un modelo de auditoría para la seguridad de infraestructuras críticas, definir procesos, controles y estrategias de gestión de riesgos. Todo esto se hace con el propósito de cumplir con la próxima actividad.

En la Tabla 32, que compara las normas con los criterios y detalla las ventajas de cada una, se destaca el Marco NIST de Ciberseguridad como el proceso que aporta el mayor valor en cada línea directriz durante la gestión de riesgos cibernéticos en auditorías. Este marco no solo proporciona pautas claras para la observación y monitoreo de recursos relevantes, sino que también establece una hoja de ruta para actualizar el modelo. Esto facilita la identificación de actividades específicas en cada fase y define roles y funciones clave para la implementación efectiva de la gestión de riesgos según la normativa.

3.2.2 Establecer las características para la ejecución de auditoría a partir de la norma seleccionada y los riesgos altos detectados

En primera instancia se realizó una comparación exhaustiva entre diversas normas, estándares y buenas prácticas con el objetivo de seleccionar de manera objetiva la más adecuada, basándonos en un sistema de puntuaciones detallado. Este proceso de evaluación implicó un análisis minucioso de los requisitos y directrices de cada marco de referencia, considerando factores críticos como la relevancia para nuestras necesidades específicas, la claridad de implementación y la efectividad en la gestión de riesgos. Al emplear un sistema de puntuaciones, se pudieron asignar ponderaciones a cada criterio, permitiendo una toma de decisiones fundamentada y transparente. Este enfoque riguroso aseguró que la norma, estándar o buenas prácticas seleccionadas no solo cumplieran con nuestros requisitos actuales, sino que también proporcionaran una base sólida para la mejora continua y la adaptabilidad a futuras evoluciones en el entorno operativo.

La definición de la metodología de auditoría se vuelve esencial al seleccionar la norma que servirá como guía fundamental para abordar la gestión de riesgos en ciberseguridad. En la (Tabla 33) se expone la metodología que orientará la elección de la norma. Esta estrategia se sustenta en el criterio de conformidad en la gestión de riesgos, constituyendo la base sólida para la realización de auditorías de ciberseguridad efectivas. El proceso se apoya en la evaluación meticulosa de cinco criterios clave que enmarcan el objetivo general, asegurando así la selección de la norma más adecuada y alineada con nuestras necesidades específicas en materia de seguridad cibernética. Este enfoque sistemático garantiza una metodología de auditoría sólida y adaptada a la dinámica y evolución constante del panorama de ciberseguridad.

Tabla 34.

Normas y Criterios de Calificación

Norma	Documentación	Auditable	Auditable para ciberseguridad	Auditable para sistema SCADA	Fácil implementación para sistemas SCADA
COSO	Amplia documentación relacionada con control interno y gestión de riesgos	Altamente auditable en términos de control interno y gestión de riesgos	Puede adaptarse a la ciberseguridad	Puede adaptarse a sistemas SCADA	Puede requerir adaptaciones específicas
COBIT	Proporciona documentación sobre la gobernanza de TI y control de procesos de TI	Altamente auditable en términos de gobernanza de TI y procesos	Relevante para la ciberseguridad	Puede adaptarse a sistemas SCADA	Puede requerir ajustes significativos

		relacionados con TI			
ITIL	Documentación extensa relacionada con la gestión de servicios de TI	Altamente auditable en términos de gestión de servicios de TI	Puede adaptarse para abordar la ciberseguridad	Centrado en la gestión de servicios de TI en general	Puede requerir adaptaciones significativas
ISO/IEC 27001	Norma específica para la gestión de seguridad de la información con documentación sólida	Altamente auditable en términos de seguridad de la información y gestión de riesgos	Relevante para la ciberseguridad	Puede adaptarse a sistemas SCADA	Puede implementarse de manera efectiva con ajustes
Marco de Ciberseguridad de NIST (CSF)	Proporciona un marco estructurado para la ciberseguridad	Altamente auditable en términos de ciberseguridad	Específicamente diseñado para ciberseguridad	Puede adaptarse a sistemas SCADA en términos de ciberseguridad	Se adapta bien a la gestión de riesgos cibernéticos en sistemas SCADA

Nota. Esta tabla presenta los criterios previos para la evaluación de cada norma.

En general, el Marco de Ciberseguridad de NIST (CSF) y la norma ISO/IEC 27001 ofrecen enfoques específicos y robustos para la gestión de riesgos de ciberseguridad en sistemas SCADA. COBIT también puede ser útil para la gestión de riesgos de TI en general en sistemas SCADA. COSO e ITIL, si bien son marcos de referencia más generales, pueden adaptarse para abordar la gestión de riesgos en sistemas SCADA con las modificaciones adecuadas.

Se asignó una clasificación según lo establecido en la Tabla 34 después de definir y evaluar los criterios para cada norma. Esta tabla proporciona la evaluación comparativa, asignando puntuaciones específicas a cada norma en función de criterios clave. Cada criterio, desde la documentación hasta la auditabilidad, se clasifica de 1 a 5 en una escala de 1 a 5. La puntuación más baja es 1 y la puntuación más alta es 5. Debido a su importancia en cualquier auditoría de seguridad y ciberseguridad, es importante destacar que los criterios "Está documentado" y "Es auditable" obtienen calificaciones elevadas en todas las normas.

Tabla 35.

Normas y Calificación de Criterios.

Criterio / Norma	ITIL	COSO	COBIT	ISO 27001	CSF NIST
Está documentado	5	5	5	5	5
Es auditable	5	5	5	5	5
Es auditable para ciberseguridad	1	1	1	5	5
Es auditable para sistema SCADA	1	1	1	1	5
Fácil implementación para sistemas SCADA	1	1	1	1	5
Fácil integración con sistemas SCADA	1	1	1	1	5
Total	14	14	14	18	30

Nota. Esta tabla presenta los resultados obtenidos en los criterios por norma y los distintos resultados.

De acuerdo con la tabla anterior, cada requisito se evalúa en términos de documentación, auditabilidad, capacidad de auditoría de ciberseguridad y aplicabilidad y facilidad de implementación e integración con sistemas SCADA. Los puntajes totales muestran el grado de cumplimiento y utilidad de cada norma o marco en relación con los requisitos de seguridad y auditoría en entornos SCADA.

El CSF del NIST obtiene la mejor puntuación, lo que demuestra su idoneidad y robustez en relación con los sistemas SCADA, así como su capacidad para abordar las necesidades de auditoría y ciberseguridad en este contexto.

En relación con los criterios específicos para ciberseguridad y sistemas SCADA, tales como "Es auditable para ciberseguridad", "Es auditable para sistema SCADA", "Fácil implementación para sistemas SCADA" y "Fácil integración con sistemas SCADA", se observa que reciben calificaciones más bajas en la evaluación. Esto se debe, en parte, a la variabilidad en la cobertura y énfasis que cada norma otorga a estos aspectos particulares. No todas las normas abordan de manera exhaustiva estos criterios, y cuando lo hacen, suelen no asignarles la misma prioridad que a los criterios más generales de documentación y auditabilidad.

Este enfoque evaluativo se resalta como esencial para guiar la elección de la norma más adecuada, teniendo en cuenta los requisitos específicos de la organización en términos de seguridad cibernética. La implementación efectiva de una estrategia de auditoría depende de una elección informada respaldada por datos concretos. La tabla de calificación, al proporcionar una visión detallada de cómo cada norma se ajusta a los criterios predefinidos, facilita la toma de decisiones al destacar las fortalezas y limitaciones de cada marco.

La complejidad de la ciberseguridad y la diversidad de los sistemas SCADA hacen que la elección de la norma adecuada sea aún más crucial. No solo se trata de cumplir con requisitos generales, sino también de abordar de manera específica los desafíos y requisitos particulares de los entornos cibernéticos y sistemas industriales. La adaptabilidad y la precisión en la elección de la norma son clave para asegurar una estrategia de auditoría efectiva y resistente ante las amenazas en constante evolución.

La auditoría de sistemas y ciberseguridad ha adquirido un papel crítico en la protección de activos digitales y la gestión de riesgos en organizaciones de todo tipo. En este contexto, la elección de una norma o marco de referencia adecuado es esencial para guiar los esfuerzos de ciberseguridad y evaluar la efectividad de los controles implementados. El Cybersecurity Framework (CSF) del Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos emerge como una opción sólida, consolidándose como un estándar de facto para numerosas organizaciones [34]. Su enfoque comprehensivo y adaptabilidad lo posiciona como una guía confiable para enfrentar los desafíos en constante evolución del panorama de ciberseguridad [61].

La elección del Marco CSF NIST se fundamenta en criterios sólidos de caracterización que lo hacen adecuado para enfrentar los desafíos de la ciberseguridad en diversos contextos organizacionales. Este marco está diseñado para ayudar a las organizaciones a identificar, proteger, detectar, responder y recuperarse de amenazas cibernéticas, proporcionando así una herramienta integral para la gestión de riesgos en ciberseguridad. Además, su flexibilidad permite a las organizaciones adaptar sus enfoques según sus necesidades específicas y evolucionar junto con el cambiante panorama de amenazas [27].

El marco CSF de NIST se construye sobre principios sólidos y las mejores prácticas de la industria, amalgamando estándares y directrices de ciberseguridad destacados, como el NIST SP 800-53 [35]. y el ISO 27001 [10] Esta integración confiere al CSF de NIST una base robusta en términos de controles y procedimientos de seguridad, asegurando que las organizaciones que optan por este marco estén alineadas con estándares ampliamente aceptados y respetados en el ámbito de la ciberseguridad.

La elección de la norma CSF NIST para la auditoría y ciberseguridad se fundamenta en criterios sólidos de caracterización y está respaldada por un marco de trabajo integral y flexible que sigue las mejores prácticas y se alinea con estándares ampliamente reconocidos. Al adoptar el CSF de NIST, las organizaciones obtienen una base sólida que les permite gestionar y mejorar de manera efectiva su postura de ciberseguridad en un entorno cada vez más desafiante y en constante evolución. Este marco no solo brinda una estructura organizativa sólida, sino que también facilita la adaptabilidad necesaria para enfrentar las dinámicas amenazas cibernéticas y mantenerse a la vanguardia de las prácticas de seguridad. La elección de este marco no solo significa alinearse con estándares reconocidos, sino también prepararse para los desafíos futuros y garantizar una seguridad cibernética resiliente.

3.2.3 Sincronización entre el marco de ciberseguridad de CSF NIST y las tres líneas de defensa de la auditoría interna

En línea con el enfoque propuesto, se avanzó hacia la integración del marco de ciberseguridad del NIST con las tres líneas de defensa de la auditoría. Este proceso de sincronización busca asegurar una implementación coherente y efectiva del marco CSF NIST en todas las capas de defensa organizativa. Al alinear el marco con las tres líneas de defensa, se fortalece la capacidad de la organización para abordar de manera integral los riesgos cibernéticos y mejorar la eficiencia en la gestión de la seguridad.

Posteriormente, se procedió a llevar a cabo la actividad planificada, que implica la integración del CSF NIST en cada línea de defensa. Este proceso permite una mayor visibilidad y coordinación en la gestión de riesgos cibernéticos en todos los niveles organizativos. La sincronización del marco con las tres líneas de defensa no solo fortalece la capacidad de respuesta ante amenazas, sino que también facilita la evaluación continua y la mejora de la postura de ciberseguridad de la organización. Este enfoque integral asegura que el marco CSF NIST no sea simplemente una herramienta aislada, sino que esté integrado de manera orgánica en la estructura de defensa de la organización, maximizando así su efectividad en la gestión de riesgos cibernéticos.

Con el fin de profundizar en el tema, se considera importante destacar que el Modelo de las Tres Líneas del Instituto de Auditores Internos (IIA), actualizado en 2020, proporciona un marco para una gobernanza y gestión de riesgos eficaces, alineándose con las prácticas modernas de control y auditoría. Este modelo destaca la importancia de la colaboración entre las diferentes funciones dentro de una organización para garantizar una sólida gestión de riesgos y control interno. Al comparar las actualizaciones del NIST 800-53 Rev. 5 con el Modelo de las Tres Líneas del IIA, se puede validar la integración de conceptos clave utilizados por el IIA [62].

1. **Primera Línea: Gestión Operacional**
    - Responsabilidad Directa: En el modelo del IIA, la primera línea está compuesta por las funciones operativas que poseen y gestionan riesgos directamente. En el NIST 800-53 Rev. 5, esto se refleja en la implementación de controles basados en resultados, donde las unidades operativas tienen la flexibilidad y responsabilidad de adaptar los controles de seguridad y privacidad según sus necesidades específicas.
    - Seguridad Adaptativa y Resiliencia: La Rev. 5 enfatiza la seguridad adaptativa y la resiliencia, aspectos cruciales para la primera línea que debe responder y recuperarse rápidamente de riesgos de seguridad, asegurando la continuidad operativa.
2. **Segunda Línea: Supervisión de Gestión de Riesgos y Cumplimiento**
    - Supervisión y Monitoreo: La segunda línea, según el IIA, proporciona supervisión y asesoría sobre la gestión de riesgos. En la Rev. 5 del NIST 800-53, los controles de privacidad y seguridad, así como la alineación con estándares internacionales, facilitan el monitoreo y cumplimiento continuo. Estos controles aseguran que las políticas y procedimientos sean adecuados y se mantengan actualizados frente a las amenazas y regulaciones emergentes.
    - Gobernanza y Políticas de Seguridad: La incorporación de la función de Gobierno en la Rev. 5 fortalece la capacidad de la segunda línea para establecer y supervisar políticas de seguridad y estrategias de ciberseguridad. Esto asegura que las decisiones de seguridad estén alineadas con los objetivos y estrategias organizacionales.

3. **Tercera Línea: Auditoría Interna**

    - Evaluación Independiente: La tercera línea, según el modelo del IIA, proporciona evaluaciones independientes de la efectividad de la gestión de riesgos y controles internos. La actualización del NIST 800-53 Rev. 5, con su enfoque en controles basados en resultados y privacidad, permite a la auditoría interna evaluar la adecuación y efectividad de estos controles, identificando áreas de mejora y asegurando el cumplimiento con las mejores prácticas y regulaciones.

    - Informe y Mejora Continua: La tercera línea también se enfoca en la mejora continua de los controles y procesos de gestión de riesgos. La Rev. 5 facilita esta función proporcionando un marco actualizado que incluye nuevos controles y mejoras en los existentes, asegurando que las prácticas de seguridad evolucionen con las amenazas y tecnologías emergentes [46].

No obstante, retomando el concepto de la tercera línea, se considera relevante destacar que aunque existe el concepto de que las auditorías, como parte de la tercera línea de defensa, no deben realizar asesorías o acompañamientos a los responsables de los procesos auditados, ya que esto podría comprometer su independencia. Sin embargo, se deja entrever que la tercera línea sí puede brindar cierto tipo de asesoría y asistencia a la gerencia en general. A continuación, se amplía el análisis sobre este punto, considerando los matices y las responsabilidades que implica:

Asesoría y asistencia permitidas:

- Asesoría general sobre riesgos y controles: La tercera línea puede brindar asesoría general a la gerencia sobre la gestión de riesgos y el diseño de controles internos. Esto puede incluir la identificación de riesgos potenciales, la recomendación de buenas prácticas y la evaluación de la eficacia de los controles existentes.

- Capacitación y sensibilización: La tercera línea puede realizar actividades de capacitación y sensibilización para la gerencia y el personal sobre temas relacionados con la gestión de riesgos, el cumplimiento y el buen gobierno corporativo.

- Comunicación de hallazgos: La tercera línea puede comunicar los hallazgos de sus auditorías y evaluaciones a la gerencia, destacando las áreas de riesgo y las oportunidades de mejora.

- Facilitación de talleres y grupos de trabajo: La tercera línea puede facilitar talleres y grupos de trabajo para la gerencia sobre temas específicos relacionados con la gestión de riesgos y el cumplimiento.

Consideraciones importantes:

- Mantener la independencia: Es crucial que la tercera línea mantenga su independencia al brindar asesoría o asistencia. Esto significa que no debe tomar partido en las decisiones de la gerencia ni presionar para que se implementen sus recomendaciones. Su rol debe ser de apoyo y facilitación, no de imposición.

- Evitar conflictos de interés: La tercera línea debe evitar cualquier situación que pueda generar un conflicto de interés. Por ejemplo, no debe brindar asesoría sobre un proceso específico que haya sido auditado por ella misma o en el que tenga intereses personales.

- Documentar las actividades: Es importante que la tercera línea documente todas las actividades de asesoría y asistencia que brinde. Esto ayudará a mantener la transparencia y a demostrar que se ha actuado de manera independiente y objetiva.

En síntesis, si bien las auditorías, como función específica dentro de la tercera línea, no deben brindar asesoría o acompañamiento directo a los responsables de los procesos auditados, la tercera línea en su conjunto sí puede jugar un rol de apoyo y asesoramiento a la gerencia en general. Al hacerlo, la tercera línea contribuye a fortalecer la cultura de gestión de riesgos y cumplimiento dentro de la organización, promoviendo así un buen gobierno corporativo. Además, es importante recordar que la clave para una asesoría y asistencia efectivas por parte de la tercera línea radica en mantener el equilibrio entre la independencia, la objetividad y el apoyo a la gerencia.

Validación de Conceptos Clave

1. Gobernanza: La función de Gobierno en el NIST 800-53 Rev. 5 resuena con la necesidad de una sólida gobernanza de riesgos destacada en el Modelo de las Tres Líneas del IIA. Asegura que las estrategias y políticas de ciberseguridad estén alineadas con los objetivos organizacionales y sean supervisadas adecuadamente.

2. Gestión de Riesgos: Tanto el NIST 800-53 Rev. 5 como el Modelo de las Tres Líneas del IIA enfatizan la importancia de una gestión de riesgos efectiva. La actualización del NIST incorpora nuevos controles que permiten una mejor identificación, evaluación y tratamiento de riesgos, facilitando el trabajo de las tres líneas de defensa.

3. Colaboración y Comunicación: La actualización del NIST 800-53 fomenta una mayor colaboración entre las funciones operativas, de supervisión y auditoría, alineándose con el enfoque del IIA sobre la necesidad de comunicación y colaboración efectiva entre las tres líneas para una gestión de riesgos integral.

En conclusión, la actualización del NIST 800-53 Rev. 5 se alinea bien con los principios del Modelo de las Tres Líneas del IIA, validando los conceptos clave de gobernanza, gestión de riesgos y auditoría interna. Al incorporar controles de privacidad, un enfoque basado en resultados y una estructura de gobernanza sólida, la Rev. 5 proporciona un marco robusto que facilita la implementación efectiva de las tres líneas de defensa, mejorando la capacidad de las organizaciones para gestionar y mitigar los riesgos de ciberseguridad de manera integral.

Tabla 36. *Integración tres líneas de auditoría y el CSF NIST*

		IMPLEMENTACION DEL FRAMEWORK CSF NIST			POST IMPLEMENTACION	
FASE	CATEGORIA	1a línea de defensa	2a línea de defensa	3a línea de defensa	Auditoria	Auditoria continua
Identificar	Gestión de activos Ambiente de negocios Gobernanza Evaluación de riesgos Estrategia de gestión de riesgos Gestión de riesgos de la cadena de suministro	Identificar y clasificar procesos de negocio, activos, riesgos y controles, basados en la estrategia de negocio y apetito de riesgos.		Asesorar y acompañar en el proceso de identificación.	Asegurar la actualización periódica basándose en eventos significativos	Alertas de altas o modificaciones de activos, riesgos o controles.
Proteger	Gestión de identidad, autenticación y Control de acceso Concienciación y capacitación Seguridad de los datos Procesos y procedimientos de protección de la información Mantenimiento Tecnología de protección	Establecer políticas, normas, procedimientos y estándares acordes a los riesgos identificados.	La segunda línea de defensa lo implementará	la tercera validará su eficiencia y efectividad.	Validar los cambios en forma periódica.	Alertas de cambios en las directivas de seguridad. Monitoreo de gestión, disponibilidad, etc.
Detectar	Anomalías y eventos Monitoreo continuo de seguridad Procesos de detección	Establecer procedimientos detección, identificación, clasificación y resolución de riesgos. Periódicamente se deben actualizar los riesgos y controles.			Verificar los riesgos críticos y que los mismos impacten en	Pistas de riesgos con tipologías, clasificaciones y riesgos asociados.

					sus procesos.	
Responder	Planificación de Respuestas Comunicaciones Análisis Mitigación Mejoras	Definir la normativa interna para cada categoría	Estratificar los riesgos ya registrados y establecer distintos planes de acción según su clasificación.	Acompañar y validar las definiciones basados en los riesgos identificados en las distintas fases.	Verificar que los riesgos se encuentren gestionados según los planes establecidos y que los mismos se encuentren actualizados	Mediciones de tiempos de respuestas ante riesgos según su taxonomía.
Recuperar	Planificación de la recuperación Mejoras Comunicaciones	Definir la normativa interna para cada categoría.	Establecer distintos planes de acción según los riesgos estratificados.	Acompañar y validar las definiciones basados en los riesgos identificados en las distintas fases.	Verificar que las mejoras implementadas mitiguen los riesgos generados por nuevos riesgos y que actualice la fase de identificación.	Mediciones de tiempos de recuperación ante riesgos según su taxonomía.

Nota: Esta tabla se presenta el resultado de integrar las tres líneas de acuerdo con el lineamiento de CSF NIST.

El análisis de la tabla 35, que integra las tres líneas de auditoría con el Marco de Seguridad Cibernética (CSF) del NIST, indica que el área de "Proteger" del CSF del NIST debe ser el foco principal. Esta decisión se basa en la comprensión de que el uso efectivo de controles de protección es esencial para reducir los riesgos de seguridad cibernética en entornos industriales.

Por otra parte, la organización puede fortalecer su enfoque en la seguridad al implementar medidas como la segmentación de redes, la autenticación robusta, el control de acceso y la encriptación de datos, entre otras. Este enfoque estratégico permite a la organización maximizar su capacidad de defensa al priorizar recursos y esfuerzos en áreas críticas de seguridad.

Fase 3: Proponer un plan de controles asociado a la reducción de los diferentes riesgos encontrados, con el fin de crear el modelo para la ejecución de auditorías.

En el transcurso de esta actividad, se procedió a la identificación y propuesta de los controles más efectivos para un sistema industrial SCADA. Este proceso tuvo en cuenta los riesgos previamente detectados en la sección de amenazas y vulnerabilidades. A continuación, se detallan los controles recomendados, estableciendo así un conjunto de medidas específicas diseñadas para mitigar y gestionar los riesgos identificados en el sistema SCADA. Esta fase de identificación y recomendación de controles es esencial para fortalecer la seguridad del sistema, proporcionando respuestas específicas a las amenazas y vulnerabilidades previamente analizadas, y contribuyendo a la creación de un entorno más resistente y protegido en el ámbito industrial.

3.3 Fase 3 Propuestas de controles para el sistema industrial SCADA

Los controles que se caracterizan a continuación están debidamente documentados en el marco del CSF del NIST. Esta elección se fundamenta en la consideración de los riesgos detallados en el mapa de riesgos, sirviendo como base sólida para su propuesta. Cada control identificado en el marco del CSF del NIST está diseñado para abordar y mitigar específicamente los riesgos previamente analizados. Esta alineación estratégica entre los controles y los riesgos mapeados garantiza una respuesta precisa y efectiva, estableciendo una estructura coherente para fortalecer la seguridad del sistema. Al seguir las directrices establecidas por el CSF del NIST, se busca no solo gestionar los riesgos de manera proactiva, sino también asegurar la implementación de medidas de seguridad robustas y adaptadas a los desafíos particulares identificados en el mapa de riesgos.

Tabla 37.

Controles según riesgos

Número	Control	Definición en base al riesgo
1	Segmentación de redes	Mitiga el riesgo de movimiento lateral de amenazas en la red al restringir el flujo de tráfico entre segmentos.
2	Autenticación fuerte	Mitiga el riesgo de acceso no autorizado a sistemas o cuentas al requerir credenciales robustas para la autenticación.
3	Control de acceso	Mitiga el riesgo de acceso no autorizado a recursos y datos sensibles al restringir el acceso a usuarios y sistemas autorizados.
4	Actualizaciones y parches	Mitiga el riesgo de explotación de vulnerabilidades conocidas en software desactualizado al aplicar parches y actualizaciones de seguridad de manera oportuna.
5	Firewalls	Mitiga el riesgo de intrusiones no autorizadas desde la red externa al filtrar el tráfico entrante y saliente.
6	Encriptación de datos	Mitiga el riesgo de exposición de datos confidenciales en caso de brechas de seguridad al encriptar los datos en reposo y en tránsito.
7	Auditoría de eventos	Mitiga el riesgo de no detectar actividades maliciosas o inusuales en la red al registrar y analizar eventos de seguridad.
8	Capacitación del personal	Mitiga el riesgo de que los empleados sean víctimas de ataques de ingeniería social al aumentar su conocimiento y conciencia sobre las amenazas cibernéticas.
9	Respuesta a incidentes	Mitiga el riesgo de no poder identificar, contener y mitigar incidentes de seguridad de manera efectiva al establecer un plan de respuesta a incidentes definido.
10	Protección física	Mitiga el riesgo de acceso físico no autorizado a sistemas críticos al implementar medidas de seguridad física como control de acceso físico y vigilancia.
11	Gestión de parches	Mitiga el riesgo de no aplicar parches críticos y exponerse a vulnerabilidades conocidas al establecer un proceso formal para la gestión de parches.

Nota. Esta tabla presenta la tipología de control de acuerdo con el concepto relacionado con riesgo.

La tabla anterior proporciona una forma estructurada de asociar controles de seguridad con los riesgos específicos que mitigan en entornos de sistemas de control industrial

(SCADA). Esta tabla es una herramienta valiosa para la gestión de riesgos en SCADA, ya que permite:

- Identificar los riesgos críticos: La tabla ayuda a identificar los riesgos más importantes que pueden afectar la seguridad y la operación de los sistemas SCADA.
- Seleccionar controles adecuados: Para cada riesgo identificado, la tabla sugiere controles de seguridad específicos que pueden mitigar ese riesgo.
- Priorizar la implementación de controles: La tabla permite priorizar la implementación de controles en función de la severidad de los riesgos asociados.
- Monitorear y evaluar la efectividad: La tabla facilita el monitoreo y la evaluación de la efectividad de los controles implementados para la gestión de riesgos.

Beneficios de la Tabla:

- Enfoque sistemático: La tabla proporciona un enfoque sistemático para la gestión de riesgos en SCADA, asegurando que se consideren todos los riesgos críticos y se implementen controles adecuados.
- Mejora en la toma de decisiones: La tabla facilita la toma de decisiones informadas sobre la selección, implementación y priorización de controles de seguridad.
- Reducción del riesgo: La implementación efectiva de los controles sugeridos en la tabla puede ayudar a reducir significativamente el riesgo de seguridad en sistemas SCADA.
- Cumplimiento normativo: La tabla puede ayudar a las organizaciones a cumplir con los requisitos de seguridad y las regulaciones aplicables a los sistemas SCADA.

Además, se ha creado un cuadro de controles clave para mejorar la seguridad de los sistemas industriales SCADA. La protección contra amenazas cibernéticas, la gestión de riesgos y la seguridad física son los objetivos de la cuidadosa selección de estos controles. Cada control que se incluye en este marco ha sido elegido estratégicamente para brindar una protección completa y equilibrada contra los diversos riesgos asociados con los entornos SCADA industriales. Esta iniciativa refleja un enfoque integral para fortalecer la seguridad, reconociendo la necesidad de medidas multifacéticas que aborden tanto las amenazas digitales como los riesgos físicos potenciales. La implementación de estos controles clave mejorará significativamente la seguridad y resiliencia del entorno SCADA.

A continuación, se proporciona una descripción concisa de cada control, junto con las referencias informativas correspondientes en el CSF del NIST.

Este cuadro se presenta como una guía completa para la implementación efectiva de medidas de seguridad en entornos SCADA. Cada control detallado en la descripción está diseñado para abordar los riesgos específicos identificados, lo que garantiza una respuesta precisa y adaptada a los desafíos del entorno industrial. Al proporcionar referencias al CSF del NIST, se garantiza que la implementación de estos controles cumpla con los estándares reconocidos en el ámbito de la ciberseguridad industrial. Este enfoque estructurado e informativo ayuda a comprender y aplicar las medidas de seguridad en entornos SCADA.

Tabla 38.

Controles según referencia CSF NIST

Número	Control	Descripción	Referencia Informativa CSF NIST
1	Segmentación de Redes	Divide la red en segmentos para limitar la propagación de amenazas y restringir el acceso a sistemas críticos.	CSF: PR.AC-4, PR.DS-4
2	Autenticación Fuerte	Requiere múltiples formas de verificación (contraseña, token, etc.) para reducir el riesgo de acceso no autorizado y suplantación de identidad.	CSF: PR.AC-7, PR.DS-5, PR.DS-6, PR.DS-7
3	Control de Acceso	Implementa políticas y mecanismos para regular el acceso a recursos y datos sensibles, previniendo el acceso no autorizado y privilegios excesivos.	CSF: PR.AC-5, PR.AC-6, PR.AC-7, PR.DS-5
4	Actualizaciones y Parches	Aplica regularmente actualizaciones y parches de seguridad para corregir vulnerabilidades conocidas y evitar interrupciones por fallos de software.	CSF: PR.IP-4, PR.IP-5, PR.IP-6
5	Firewalls	Controla y filtra el tráfico de red para prevenir intrusiones no autorizadas y proteger contra tráfico malicioso.	CSF: PR.DS-4, PR.DS-5, PR.DS-6, PR.DS-7
6	Encriptación de Datos	Protege información confidencial convirtiéndola en un formato ilegible, evitando exposición de datos en caso de brechas.	CSF: PR.DS-3, PR.DS-4, PR.DS-6, PR.DS-7
7	Auditoría de Eventos	Monitorea y registra actividades en la red para detectar comportamientos maliciosos o inusuales, cumpliendo con requisitos regulatorios.	CSF: PR.DS-1, PR.DS-2, PR.DS-3, PR.DS-6, PR.DS-7
8	Capacitación del Personal	Proporciona educación regular sobre seguridad informática para concientizar a los empleados sobre amenazas y tácticas de ingeniería social.	CSF: PR.AT-1, PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, PR.AT-6, PR.AT-7
9	Respuesta a Riesgos	Desarrolla un plan para identificar, contener y mitigar riesgos de seguridad, incluyendo simulacros para evaluar la capacidad de respuesta.	CSF: PR.RP-1, PR.RP-2, PR.RP-3, PR.RP-4, PR.RP-6
10	Protección Física	Implementa medidas de seguridad física, como controles de acceso y vigilancia, para prevenir acceso físico no autorizado y proteger la infraestructura.	CSF: PR.PT-1, PR.PT-2, PR.PT-3, PR.PT-4, PR.PT-5, PR.PT-6
11	Gestión de Parches	Establece un proceso para aplicar parches críticos de manera oportuna, evitando la exposición a vulnerabilidades conocidas e interrupciones no planificadas.	CSF: PR.IP-4, PR.IP-5, PR.IP-6

Nota. Esta tabla presenta la descripción detallada de controles según referencia 3, 5,7,10.

La tabla incluye una lista de controles de seguridad para entornos industriales, cada uno de los cuales está acompañado de una descripción detallada y su correspondencia con los componentes del Marco de Seguridad Cibernética (CSF) de NIST. Estos controles cubren una variedad de aspectos importantes de seguridad, incluida la segmentación de redes y la autenticación robusta, así como la gestión de parches y la capacitación del personal. Cada control asignado a los componentes específicos del CSF del NIST resalta su importancia para los pilares fundamentales de la seguridad cibernética: identificación, protección, detección, respuesta y recuperación. Esto proporciona directrices claras para el diseño e implementación de medidas de seguridad industriales efectivas, lo que ayuda a las organizaciones a fortalecer sus defensas contra amenazas cibernéticas y cumplir con los controles.

3.3.1 Construcción del modelo de auditoría de seguridad para sistemas industriales SCADA

En la etapa de preparación, el modelo de ejecución de auditoría recomienda definir conceptos y definiciones clave. Esto requiere la integración del marco de ciberseguridad de NSIT y la auditoría, así como el ciclo de vida evolutivo de Deming. Estos componentes son necesarios para que el modelo funcione correctamente. La definición de ciberseguridad se retomó en las siguientes etapas porque sirvió como base para la selección de la norma y la auditoría de ciberseguridad. Como resultado, se incluyó la definición fundamental de auditoría en relación con la auditoría de ciberseguridad. Por último, se mejoró la comprensión de la relevancia de la auditoría interna como un componente crucial en el ámbito de la ciberseguridad. Este método

Ciberseguridad: Es la sinergia de tecnologías, procesos y prácticas, que permiten proteger la información, las redes, los sistemas, aparatos electrónicos y los programas utilizados para recopilar, procesar, almacenar y proteger la información, de ataques, daños y accesos no autorizado.

se preocupa por proteger todo lo que está dentro de una red, hardware, software e información, que es procesada y almacenada dentro de un sistema aislado o transportado por ambientes interconectados.

Con respecto a los fundamentos de auditoria se basó en los siguientes conceptos:

Gobernabilidad:

- Responsabilidad del Directorio y Management.
- Provee dirección estratégica en Ciberseguridad.
- Asegura el cumplimiento de los objetivos.
- Verifica que el riesgo está siendo administrado adecuadamente.
- Verifica que los recursos son usados adecuadamente.

Riesgo:

- La identificación, análisis, priorización y administración de los riesgos.
- Es necesario definir el apetito al riesgo en ciberseguridad.

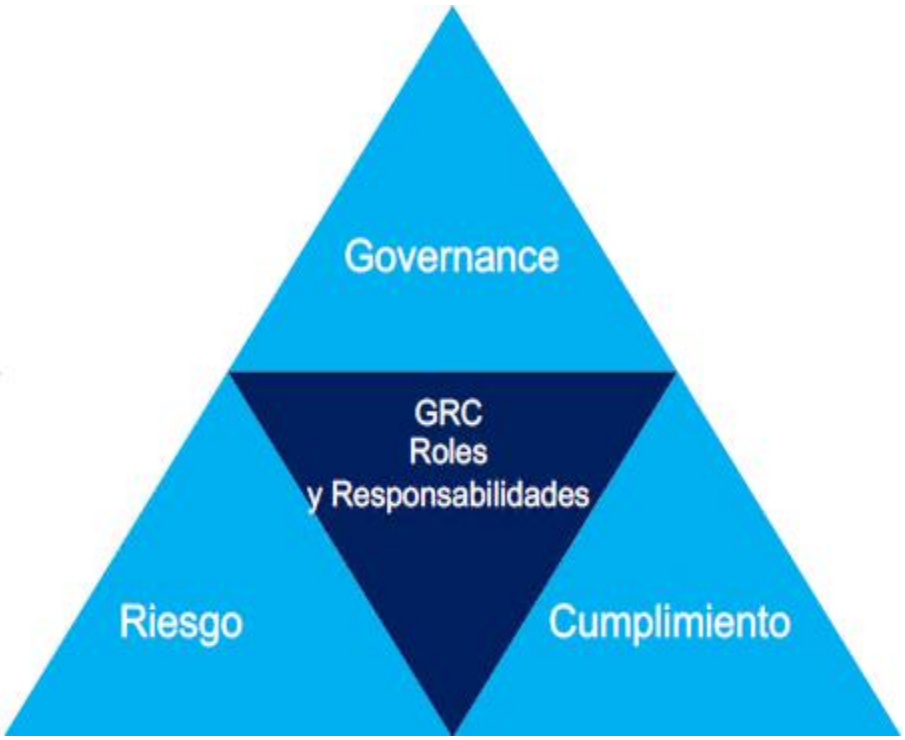
- Las organizaciones para administrar los riesgos de ciberseguridad deben implementar controles.

Cumplimiento:

- Leyes, estándares, regulaciones.
- Interno y externo [25]

Figura 15.

Fundamentos de la auditoria.



Nota. Esta figura explica detalladamente Fundamentos de la auditoria. adaptado de Instituto Nacional de Estándares y Tecnología NIST, Marco para la mejora de la seguridad cibernética en, 2018.

Primera Línea Defensa:

- La gerencia asume la responsabilidad por los temas de Ciberseguridad y delega la responsabilidad en funciones especializadas.
- Los controles, métricas, indicadores y revisiones periódicas sirven como un instrumento para identificar debilidades.
- Identifica las mejoras en Ciberseguridad que son requeridas para proteger el activo digital de la organización.
- Segunda Línea Defensa:

- La segunda línea de defensa con la primera línea de defensa, aseguran que los riesgos de Ciberseguridad son identificados, entendidos, documentados y mitigados a través del diseño e implementación de controles.

Tercera Línea Defensa:

- Evaluación independiente en los aspectos de pruebas y aseguramiento [27].

Posteriormente, otros conceptos para tener en cuenta para crear nuestro modelo son:

Auditoría en Ciberseguridad: Provee a la administración una visión independiente de la efectividad de los procesos (las políticas, procedimientos, gobernabilidad y otros controles), personas y tecnologías que asociadas a Ciberseguridad.

Personas:

- Profesionales experimentados
- Profesionales Certificados

Procesos:

- Gestión de Políticas
- Cultura en Ciberseguridad
- Gestión de Vulnerabilidades
- Inteligencia de Amenazas
- Gestión de Riesgos y Cibercrisis
- Otros

Tecnología:

- Software A/V, A/M
- SOC/SIEM
- Software EndPoint
- Otros

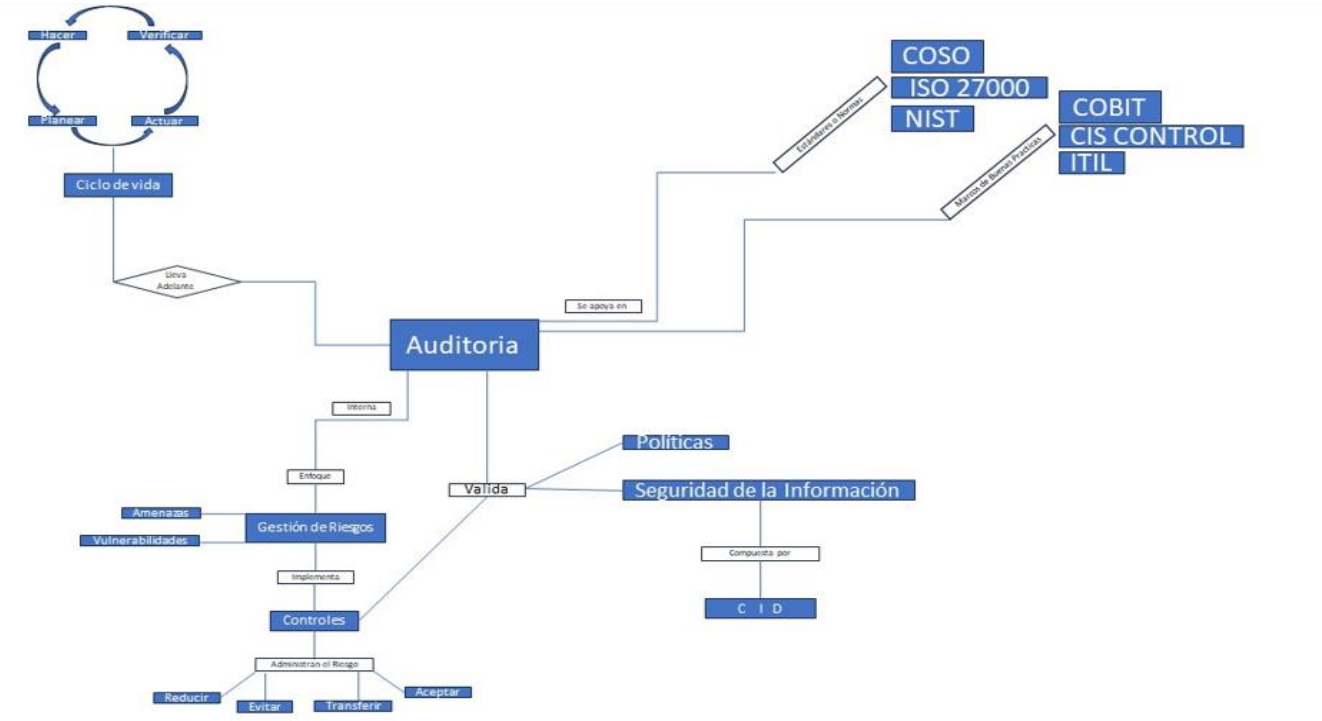
En la creación del modelo de auditoría de seguridad para entornos industriales SCADA, se llegó a la conclusión de que dicho modelo se fundamenta en la ciberseguridad. Esto se debe a su énfasis en dispositivos electrónicos presentes dentro de un sistema aislado o transportados a través de entornos interconectados. La interdependencia de estos dispositivos en ambientes industriales críticos subraya la importancia de la ciberseguridad como elemento central del modelo propuesto. El enfoque específico en la seguridad de estos sistemas, que abarcan desde dispositivos electrónicos aislados hasta aquellos inmersos en entornos interconectados, resalta la necesidad de medidas específicas y adaptadas para garantizar la integridad y protección de estos sistemas críticos. La base 02 cibernética del modelo de auditoría refleja una respuesta anticipada y especializada a los desafíos que presentan los entornos industriales SCADA en la actualidad.

3.3.2 Creación del modelo de auditoria

En el proceso de creación de este modelo, se optó por mencionar dos aspectos importantes a nivel teórico: las buenas prácticas del CSF del NIST y la norma ISO 19011 para auditoría. Este enfoque se fundamenta en la necesidad de alinear el modelo con estándares reconocidos que aborden tanto la seguridad cibernética como las mejores prácticas de auditoría. La integración del ciclo evolutivo de Deming en cada proceso, desde la gestión de riesgos hasta la auditoría y el marco CSF del NIST, establece una conexión holística y sinérgica. Este enlace estratégico garantiza que cada componente contribuya de manera coherente a la robustez del modelo y su capacidad para abordar los desafíos de seguridad en entornos industriales.

Figura 16.

Conceptos de auditoría y el ciclo de vida



Nota. Esta figura explica detalladamente el proceso de ciclo de vida mediante conceptos adaptado de Instituto Nacional de Estándares y Tecnología NIST, Marco para la mejora de la seguridad cibernética en, 2018.

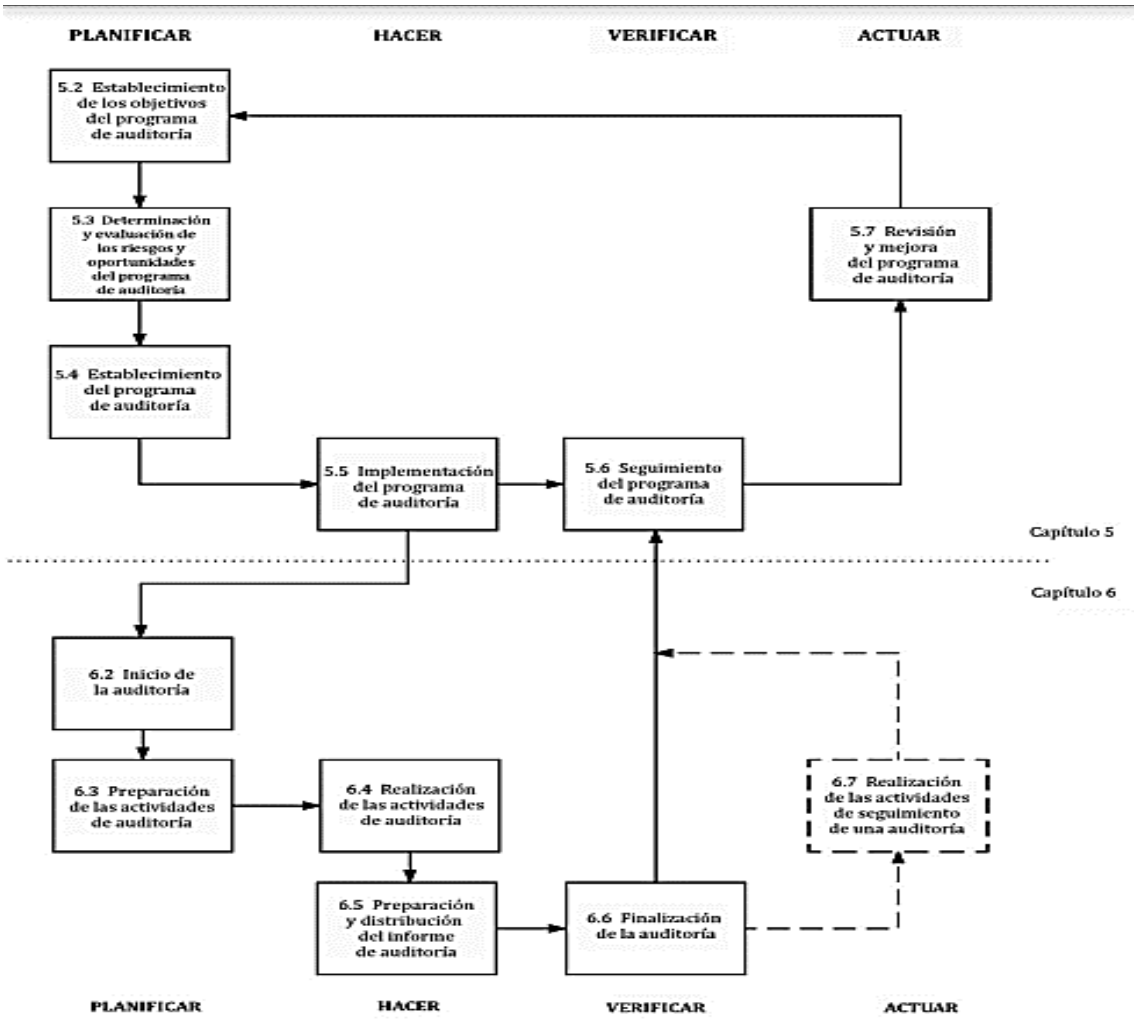
Para respaldar y validar de manera más efectiva la perspectiva del modelo, se documentó una fuente adicional: la norma ISO 19011 para auditoría. Esta norma proporciona un marco sólido para comprender la importancia del ciclo de vida y su implementación práctica mediante criterios específicos de auditoría.

De esta manera, la Figura 16 destaca visualmente la interrelación entre los conceptos de auditoría y el ciclo de vida, proporcionando una guía visual para los profesionales involucrados en la implementación del modelo. Esta conexión entre la teoría y la práctica

refuerza la base conceptual del modelo y su capacidad para adaptarse a diferentes contextos y necesidades de seguridad.

Figura 17.

Secretaría Central de ISO, 2018



Nota. Esta figura explica todos los procesos de la Secretaría Central de ISO, 2018 adaptado de Instituto Nacional de Estándares y Tecnología NIST, Marco para la mejora de la seguridad cibernética en, 2018.

La Figura 17, proveniente de la Secretaría Central de ISO en 2018, presenta un gráfico de flujo que se centra en la administración de un programa de auditoría. Este diagrama destaca las etapas del proceso dispuestas según el ciclo PDCA, lo que refleja la aplicación práctica de las directrices de la norma ISO 19011. La interconexión estratégica entre las buenas prácticas, el ciclo de Deming y la norma ISO 19011 proporciona un marco sólido y adaptable para la creación y ejecución del modelo de auditoría. Esta alineación con estándares internacionales refuerza la validez y la eficacia del modelo en la mejora continua de la seguridad en entornos industriales SCADA.

Finalmente, se utilizaron los niveles de implementación del marco de ciberseguridad de NIST para evaluar la madurez del modelo de auditoría. Esta elección se debe a la expansión y solidez del marco NIST, que ofrece pautas detalladas para mejorar la ciberseguridad de las empresas. Los Niveles de implementación, que van desde el Nivel 1 (Inicial) hasta el Nivel 4 (Adaptativo), ofrecen un marco escalonado para evaluar la sofisticación y eficacia de la implementación de medidas de ciberseguridad. Al conectar el modelo de auditoría con estos niveles, se establece un punto de referencia claro para medir la madurez de la seguridad en entornos industriales SCADA. Esta estrategia ayuda a la autoevaluación.

La integración con los Niveles de Implementación del Marco de Ciberseguridad del NIST permite una evaluación de la madurez del modelo de auditoría y su capacidad para abordar los desafíos dinámicos de la ciberseguridad industrial. La evaluación basada en estos niveles proporciona un método sistemático y progresivo para evaluar la efectividad de las medidas de seguridad implementadas. Para ello la Tabla 38 representa los Niveles de Implementación del Marco de Ciberseguridad de NIST, el modelo de auditoría demuestra su adherencia a las mejores prácticas y su capacidad para adaptarse a los cambios constantes en el panorama de amenazas cibernéticas en entornos SCADA, al alinearse con los estándares internacionalmente reconocidos.

Tabla 39.

Niveles de Implementación del Marco de Ciberseguridad del NIST

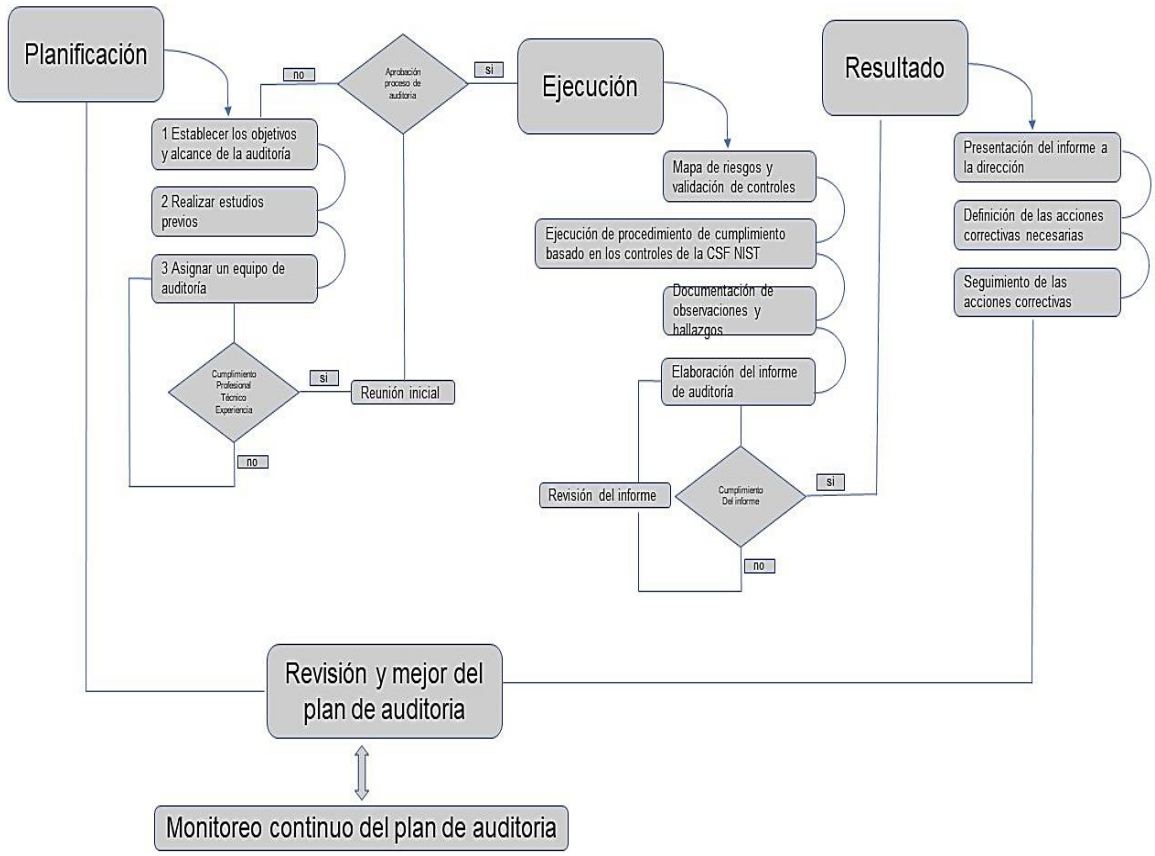
NIVEL	PROCESO DE GESTIÓN DE RIESGOS	PROGRAMA INTEGRADO DE GESTIÓN DE RIESGOS	PARTICIPACIÓN EXTERNA
1 PARCIAL	Las prácticas de gestión de riesgos de seguridad cibernética no están formalizadas, en ocasiones se hace de forma reactiva	Hay poco conocimiento en la organización del riesgo de ciberseguridad, incluso, la gestión de este puede hacerse de manera irregular	En general la organización desconoce los riesgos cibernéticos de su cadena de suministro y no recibe ni comparte información con otras entidades para gestionar la ciberseguridad.
2 RIESGO INFORMADO	Aunque hay prácticas de gestión aprobados por la dirección es posible que no se establezcan como políticas para toda la organización.	Se tiene conciencia sobre el riesgo de seguridad cibernética, sin embargo, no hay un enfoque definido para gestionar, es más, la información sobre esto se comparte informalmente.	La empresa es consciente de los riesgos cibernéticos de la cadena de suministro, pero no actúa formalmente sobre estos.

3 REPETIBLE	Las prácticas de gestión de riesgos de ciberseguridad están aprobadas y son políticas, además, se actualizan periódicamente.	Toda a organización está enfocada en gestionar el riesgo cibernético, se tienen métodos para responder de manera oportuna y efectiva a los cambios que pueda tener y os encargados comunican regularmente sobre este.	La organización contribuye a la comprensión de los riesgos cibernéticos por parte de la comunidad, colabora y recibe información de otras entidades. También comparte y actúa formalmente sobre los riesgos cibernéticos de la cadena de suministro
4 ADAPTABLE	Adapta sus prácticas de ciberseguridad de acuerdo con actividades previas y lecciones aprendidas, además, es capaz de responder eficazmente a los nuevos riesgos y amenazas.	La organización está preparada paro gestionar el riesgo cibernético y abordar posibles eventos de este tipo, Este riesgo Es considerado igual de importante que otros riesgos a los que está expuesta.	Comparte información con otras entidades, además, actúa en tiempo real -o casi real- para comprender y tomar acciones oportunas sobre los riesgos cibernéticos de la cadena de suministro.

Nota. Esta tabla explica todos los niveles de requerimientos necesarios para Implementación del Marco de Ciberseguridad del NIST. Adaptado a partir de NIST., Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, vol. 05, 2021, pp. 61-72.

Figura 18.

Modelo de auditoria



Nota. Esta figura explica como está conformado el Modelo para la Ejecución de Auditoría de Seguridad en Entornos Industriales SCADA.

La información proporcionada anteriormente sirvió como base sólida para establecer el modelo destinado a la ejecución de auditorías de seguridad en entornos industriales SCADA. Este modelo se presenta visualmente en la Figura 18, que representa la estructura integral diseñada para guiar y optimizar el proceso de auditoría. La representación gráfica del modelo ofrece una visión clara y concisa de los componentes clave, sus interrelaciones y el flujo secuencial de actividades. Al presentar el modelo de manera visual, se facilita su comprensión y aplicación por parte de los profesionales involucrados en el ámbito de la seguridad industrial.

De acuerdo con la figura anterior, se definen los criterios evaluativos los cuales estuvieron orientados en el modelo de auditoría para entornos industriales SCADA. Para establecer un marco estructurado para asi garantizar la ejecución desde el contexto académico en la implementación del modelo, son necesarias estas definiciones. Cada criterio evaluado fue discutido teniendo en cuenta los niveles técnicos mencionados en la teoría, incluidos sus componentes constitutivos, características principales y relevancia para la evaluación de seguridad. Esta clarificación terminológica permite a los auditores y otros profesionales

realizar evaluaciones rigurosas y efectivas, lo que aumenta la transparencia y la precisión del proceso evaluativo.

Finalmente hay que destacar que los sistemas de control y adquisición de datos industriales (SCADA) son componentes críticos de la infraestructura crítica, controlando procesos esenciales en sectores como la energía, el transporte y la manufactura. La creciente sofisticación de las amenazas cibernéticas resalta la necesidad de contar con modelos de auditoría de seguridad robustos y confiables para proteger estos sistemas [63].

- **Enfoque basado en estándares reconocidos**

El modelo de auditoría de seguridad para sistemas SCADA presentado en este trabajo se basa en dos marcos de referencia ampliamente reconocidos:

- **Buenas prácticas del NIST Cybersecurity Framework (CSF):** El CSF proporciona una guía estructurada para la gestión de riesgos cibernéticos, permitiendo la identificación, análisis y priorización de las amenazas potenciales en entornos SCADA.

- **Norma ISO 19011 para auditoría:** Esta norma establece principios y directrices para la realización de auditorías de calidad, asegurando la objetividad, independencia y profesionalismo del proceso de auditoría.

La integración de estos dos marcos proporciona una base sólida para el modelo, garantizando su efectividad en la identificación, evaluación y mitigación de riesgos cibernéticos en entornos SCADA.

- **Ciclo evolutivo de Deming para la mejora continua**

El modelo incorpora el ciclo evolutivo de Deming, un enfoque de mejora continua que implica las siguientes etapas:

1. Planificar: Establecer objetivos y definir el alcance de la auditoría.
2. Hacer: Realizar la auditoría de acuerdo con el plan establecido.
3. Verificar: Evaluar los resultados de la auditoría e identificar áreas de mejora.
4. Actuar: Implementar las acciones correctivas y preventivas identificadas.

La aplicación del ciclo de Deming promueve la revisión y actualización constante del modelo, asegurando que se adapte a las nuevas amenazas y a las mejores prácticas emergentes en materia de ciberseguridad industrial.

- **Evaluación basada en los Niveles de Implementación del Marco de Ciberseguridad del NIST**

El modelo de auditoría de seguridad para sistemas SCADA se alinea con los Niveles de Implementación del Marco de Ciberseguridad del NIST, permitiendo evaluar la madurez del modelo y su capacidad para abordar los desafíos dinámicos de la ciberseguridad industrial. Esta evaluación sistemática y progresiva proporciona una herramienta valiosa para medir la efectividad de las medidas de seguridad implementadas y para identificar áreas de mejora continua.

En conclusión el modelo de auditoría de seguridad para sistemas industriales SCADA presentado en este documento ofrece un enfoque robusto y completo para la gestión de riesgos cibernéticos en entornos SCADA. Su sólida base teórica, la integración de marcos de referencia reconocidos y la aplicación del ciclo evolutivo de Deming lo convierten en una herramienta invaluable para las organizaciones que buscan proteger sus activos críticos y garantizar la continuidad operativa.

- **Fortalezas del modelo:**
- Enfoque basado en estándares reconocidos: El modelo se basa en dos marcos de referencia ampliamente aceptados, lo que garantiza su confiabilidad y validez.

- Ciclo evolutivo de Deming: La aplicación del ciclo de Deming promueve la mejora continua del modelo y su adaptación a las nuevas amenazas.

- Evaluación basada en los Niveles de Implementación del Marco de Ciberseguridad del NIST: Permite medir la madurez del modelo y su capacidad para abordar los desafíos dinámicos de la ciberseguridad industrial.

- **Aplicación Concreta del NIST 800-53 y el NIST CSF en Sistemas Industriales**

La industria moderna depende en gran medida de los sistemas de control industrial (ICS) y los sistemas de adquisición de datos (SCADA) para operar de manera segura y eficiente. Sin embargo, estos sistemas son cada vez más vulnerables a los ataques cibernéticos, lo que puede tener consecuencias graves, que incluyen:

- Pérdida de producción: Las interrupciones del sistema pueden causar pérdidas significativas de producción y costos financieros.

- Daños a la propiedad: Los ataques cibernéticos pueden dañar físicamente la infraestructura industrial, lo que puede provocar daños a la propiedad y riesgos para la seguridad.

- Robo de datos: Los sistemas SCADA pueden contener información confidencial, como datos de procesos industriales o propiedad intelectual, que pueden ser robados por actores maliciosos.

Para abordar estos riesgos, es fundamental implementar un enfoque robusto de gestión de riesgos de ciberseguridad en los entornos industriales. Los estándares NIST 800-53 y NIST CSF proporcionan marcos de referencia valiosos para la evaluación y gestión de riesgos de ciberseguridad en sistemas SCADA.

- **Aplicación del NIST 800-53 en Sistemas SCADA:**

El NIST 800-53 proporciona una guía para la realización de evaluaciones de riesgo de seguridad de la información. En el contexto de los sistemas SCADA, esta guía se puede aplicar para:

- Identificar activos: Inventariar todos los componentes de los sistemas SCADA, incluyendo hardware, software, redes y datos.

- Evaluar amenazas y vulnerabilidades: Analizar las amenazas potenciales y las vulnerabilidades existentes en los sistemas SCADA.
- Estimar el impacto: Determinar el impacto potencial de los riesgos de seguridad en los sistemas SCADA.
- Priorizar riesgos: Clasificar los riesgos de seguridad en función de su probabilidad y severidad.
- Seleccionar controles: Identificar e implementar controles de seguridad adecuados para mitigar los riesgos de seguridad.

- **Patrones de controles de seguridad basados en NIST 800-53 para sistemas SCADA:**
  - Control de acceso: Implementar mecanismos de control de acceso para restringir el acceso a los sistemas SCADA solo a usuarios autorizados.
  - Protección de redes: Segmentar las redes SCADA y utilizar firewalls para protegerlas de accesos no autorizados.
  - Monitoreo y detección de intrusiones: Implementar sistemas de monitoreo para detectar actividades sospechosas y ataques cibernéticos.
  - Copia de seguridad y recuperación: Realizar copias de seguridad regulares de los datos de los sistemas SCADA y tener planes de recuperación en caso de riesgos.
  - Gestión de parches: Aplicar parches de seguridad de manera oportuna para corregir vulnerabilidades conocidas.

- **Alineación con el NIST CSF:**

El NIST CSF es un marco de referencia para la gestión de riesgos de ciberseguridad que proporciona una visión integral de las actividades necesarias para proteger los sistemas de información. En el contexto de los sistemas SCADA, el NIST CSF se puede utilizar para:

- Establecer una estrategia de gestión de riesgos: Definir una estrategia general para la gestión de riesgos de ciberseguridad en los sistemas SCADA.
- Implementar controles: Asegurar que los controles de seguridad implementados estén alineados con los principios y categorías del NIST CSF.
- Monitorear y medir la efectividad: Monitorear el desempeño de los controles de seguridad y medir la efectividad general de la estrategia de gestión de riesgos.

Paradigma de alineación del modelo de auditoría con el NIST CSF:

- **Fase de planificación:** Alinear los objetivos de la auditoría con los objetivos estratégicos de gestión de riesgos de ciberseguridad de la organización.
- **Fase de ejecución:** Vincular las actividades de auditoría con las actividades relevantes del NIST CSF, como la identificación de activos, la evaluación de riesgos y la implementación de controles.

- **Fase de informes:** Presentar los hallazgos de la auditoría en un formato que sea compatible con el marco de NIST CSF, facilitando la comparación con otras evaluaciones y la toma de decisiones.

3.4 Fase 4. Validación del modelo

3.4.1 Creación de un caso de estudio

Título del Caso de Estudio:

"Validación de un Modelo de Auditoría de Seguridad en Sistemas Industriales SCADA utilizando Buenas Prácticas Internacionales: Un Enfoque Práctico"

Objetivo del caso de estudio: El objetivo del presente caso de estudio es aplicar y validar un modelo de auditoría de seguridad en un entorno hipotético de un sistema industrial SCADA con controles de seguridad insuficientes, políticas basadas en manuales de usuario de dispositivos y contraseñas por defecto. Se busca demostrar la efectividad del modelo en la identificación y mitigación de riesgos. Dado que los sistemas SCADA desempeñan un papel crítico en entornos industriales, la aplicación de este modelo busca fortalecer la seguridad de estos sistemas, garantizando que cumplan con los estándares de seguridad globalmente reconocidos.

Introducción: La seguridad en los sistemas industriales SCADA es crucial para garantizar el funcionamiento seguro y confiable de las operaciones industriales. Estos sistemas son fundamentales en la supervisión y control de procesos críticos, como la generación de energía, el suministro de agua, la producción industrial y más. La interconexión creciente de estos sistemas con redes y la expansión de amenazas cibernéticas ha elevado la importancia de salvaguardar la integridad y la disponibilidad de los sistemas SCADA. En este caso de estudio, se presenta un modelo que combina el marco de ciberseguridad de la NIST en auditoría de seguridad. El objetivo principal de este modelo es fortalecer la seguridad de los sistemas SCADA en las empresas, garantizando que cumplan con los estándares de seguridad globalmente reconocidos y reduciendo el riesgo de exposición a ciberataques que podrían tener un impacto significativo en la infraestructura industrial y la seguridad pública. Este caso de estudio proporcionará una evaluación crítica de la efectividad de este modelo, su implementación y sus beneficios para la seguridad y la continuidad de las operaciones industriales.

El contexto de Colombia ha estado marcado por períodos de inestabilidad y desafíos, y en este marco, se examinan cinco ciberataques que han adquirido notoriedad en los medios de comunicación. Estos casos se presentan como ejemplos representativos de un espectro más amplio de eventos que a menudo pasan desapercibidos pero que merecen análisis. El objetivo es comprender en detalle algunos de los riesgos, basándose en información de acceso público, y a partir de esta revisión, identificar tendencias sectoriales y extraer lecciones clave. Estos eventos ilustran el impacto que pueden tener en sectores diversos y críticos de la sociedad, como el de la salud (Ataque al Invima), el proceso electoral (Ataque Registraduría Nacional del Estado Civil), los medios de comunicación (Ataques a Caracol Noticias y Blu

Radio), la seguridad de la información (Ataque Keralty-Colsánitas), y la infraestructura de servicios públicos (Ataque a EPM). Cada uno de estos casos subraya la importancia de la seguridad cibernética y la necesidad de estar preparados para abordar los retos que plantea en el futuro.

El alcance: de este caso de estudio se concentra en la auditoría de seguridad de un sistema industrial SCADA en una planta de generación de energía, priorizando la evaluación de componentes críticos como los controladores lógicos programables (PLC), las interfaces hombre-máquina (HMI) y la red de comunicación. Este enfoque estratégico permite una revisión exhaustiva de áreas fundamentales para la operación segura de la planta, identificando vulnerabilidades y debilidades que podrían comprometer su integridad. Al limitar el alcance a estos elementos esenciales, se facilita el análisis detallado y la implementación de medidas de seguridad efectivas para garantizar la continuidad y confiabilidad de la generación de energía, contribuyendo a la seguridad energética y al bienestar de la sociedad en su conjunto.

El contexto: La empresa hipotética llamada "EnerCorp" adquiere una importancia crítica en la industria de la generación de energía, ya que desempeña un papel esencial en la provisión de un suministro eléctrico confiable a una extensa área metropolitana. "EnerCorp" se encuentra en la vanguardia de la producción de energía, destacándose como un actor clave en la satisfacción de las crecientes demandas energéticas de la región. Su sistema SCADA, que corresponde al acrónimo de Supervisory Control and Data Acquisition, representa la infraestructura tecnológica central que coordina las operaciones críticas relacionadas con la generación, distribución y mantenimiento de la infraestructura eléctrica. Este sistema habilita la supervisión en tiempo real de múltiples puntos de generación y permite la regulación de la producción de energía para cumplir con las cambiantes demandas del área metropolitana. Sin embargo, es importante destacar que "EnerCorp" presenta una carencia significativa en lo que respecta a la seguridad, ya que carece de controles de seguridad efectivos, dependiendo únicamente de los manuales del dispositivo y políticas mínimas, incluyendo contraseñas por defecto y débiles. La seguridad y la eficiencia de este sistema SCADA son elementos críticos para garantizar la estabilidad energética de la región y, por ende, el bienestar de la comunidad. En este contexto, se plantea la implementación de un modelo de auditoría de seguridad con el propósito de elevar el nivel de madurez en lo que concierne a la seguridad informática, partiendo de la situación actual de "EnerCorp".

La infraestructura TIC: EnerCorp se compone de una serie de elementos críticos que desempeñan un papel fundamental en la operación de la planta. Los Controladores Lógicos Programables (PLC), distribuidos estratégicamente en diversas secciones de la planta, representan el núcleo de automatización y control de procesos. Estos dispositivos son esenciales para la gestión de equipos y maquinaria, así como para la supervisión de variables críticas en tiempo real. La red de comunicación de EnerCorp, basada en protocolos industriales como Modbus TCP, establece un robusto entramado que conecta los PLC, permitiendo la transmisión de datos y comandos vitales para el funcionamiento eficiente y seguro de la planta. Esta red garantiza una coordinación sin fisuras entre los diferentes componentes del sistema SCADA. Además, la estación centralizada de Interfaz Hombre-Máquina (HMI) actúa como la ventana a través de la cual los operadores y técnicos acceden y supervisan el estado de la planta en tiempo real. Facilita la toma de decisiones informadas

y la respuesta rápida ante cualquier eventualidad, al brindar una representación gráfica y datos en tiempo real de la operación de la planta. La conjunción de estos elementos en la infraestructura TIC de EnerCorp es fundamental para garantizar la eficiencia operativa, la seguridad y la confiabilidad en la generación de energía eléctrica, y, por ende, para mantener el suministro energético en el área metropolitana en condiciones óptimas.

La problemática: EnerCorp se enfrenta de suma relevancia al entorno de la seguridad cibernética y tiene implicaciones directas en la integridad y continuidad de sus operaciones críticas. Entre las preocupaciones identificadas, destaca la necesidad de abordar posibles vulnerabilidades en la configuración de los Controladores Lógicos Programables (PLC), que constituyen un componente clave en el sistema SCADA de la planta. Estas vulnerabilidades potenciales podrían ser explotadas por actores malintencionados para acceder y manipular el control de los procesos, lo que podría desencadenar fallas significativas en la generación de energía.

Además, la falta de autenticación robusta y cifrado en las comunicaciones, especialmente en una red de comunicación que utiliza protocolos industriales como Modbus TCP, representa un riesgo importante. La transmisión de datos no cifrados podría exponer la planta a escuchas no autorizadas y manipulación de la información transmitida, lo que pone en peligro la confidencialidad e integridad de los datos críticos de operación.

Por último, la implementación de políticas de acceso inadecuadas aumenta el riesgo de accesos no autorizados al sistema SCADA, lo que podría dar lugar a interrupciones no planificadas en la generación y distribución de energía eléctrica. La necesidad de establecer políticas de acceso sólidas y una autenticación rigurosa se vuelve imperativa para mitigar estos riesgos y proteger la infraestructura eléctrica y la continuidad de servicio.

Resolver estas cuestiones de seguridad es esencial para salvaguardar la operación ininterrumpida de EnerCorp y garantizar la confiabilidad de su suministro energético en el área metropolitana. El abordaje de estas problemáticas representa un paso crítico hacia el fortalecimiento de la ciberseguridad y la protección de los sistemas SCADA en un entorno de generación de energía de importancia estratégica.

Las expectativas: En términos de fortalecer la postura de seguridad de EnerCorp, se llevará a cabo una auditoría de seguridad utilizando el modelo propuesto. En primer lugar, se espera que esta auditoría descubra cualquier falla o falla potencial en el sistema SCADA de la empresa. Este análisis proporcionará una comprensión profunda de los puntos potenciales de exposición a riesgos, ya sean internos o externos, y una visión detallada de las áreas que requieren atención inmediata. Además, se espera que la auditoría produzca sugerencias claras y prácticas para mejorar la seguridad del sistema. Las mejores prácticas y estándares internacionales respaldarán estas recomendaciones, lo que garantizará un enfoque sólido y efectivo para abordar los desafíos de seguridad. Para garantizar la disponibilidad e integridad de la información crítica transmitida en la red, se espera que se implementen técnicas de autenticación fuertes que refuercen la identificación y verificación de usuarios y dispositivos, así como el cifrado de datos.

3.4.2 Validación del modelo de auditoria

La validación del modelo de auditoría representa un paso crucial en el proceso de asegurar la efectividad y confiabilidad de las prácticas de auditoría de seguridad en cualquier entorno organizacional. Este proceso implica la evaluación y verificación de un modelo propuesto de auditoría, con el fin de garantizar que cumple con los objetivos y estándares previamente establecidos. En este contexto, se explora la importancia de la validación del modelo de auditoría como una etapa esencial para asegurar la robustez de las evaluaciones de seguridad, identificar las amenazas y vulnerabilidades garantizando la adhesión a mejores prácticas y estándares internacionales. Este texto introductorio proporcionará una visión general de los principios fundamentales involucrados en el proceso de validación del modelo de auditoría y su relevancia en el ámbito de la seguridad cibernética y la gestión de riesgos.

3.4.3 Planificación de la auditoría

Objetivo: El objetivo fundamental de esta auditoría de seguridad en el sistema SCADA de EnerCorp radica en la evaluación de los controles de seguridad existentes. Esto implica un examen de las políticas, procedimientos, dispositivos y prácticas implementadas en el sistema, con el propósito de determinar su eficacia en la protección de la infraestructura crítica de generación de energía. La evaluación se centra en identificar posibles vulnerabilidades y debilidades que podrían exponer el sistema a amenazas cibernéticas, fallas operativas o cualquier otro evento que pueda poner en riesgo la integridad y disponibilidad de la infraestructura eléctrica. (para más detalle ver Anexo 2).

Este proceso no se limita a la identificación de problemas, sino que también tiene un enfoque proactivo al proponer recomendaciones sólidas y prácticas para mejorar la seguridad. Estas recomendaciones se basan en mejores prácticas reconocidas a nivel internacional y en estándares de seguridad cibernética, como la implementación de autenticación fuerte, cifrado de datos, políticas de acceso basadas en roles, entre otros. El objetivo final es fortalecer la protección de la infraestructura crítica y garantizar la continuidad de las operaciones de generación de energía de EnerCorp en un entorno de crecientes amenazas cibernéticas y desafíos de seguridad. La auditoría representa un paso esencial para mantener la integridad de la infraestructura crítica y asegurar un suministro de energía eléctrica confiable para la comunidad en general.

Alcance: La auditoría planificada se centrará en la evaluación del sistema SCADA utilizado en la planta de generación de energía de EnerCorp, abarcando los componentes de hardware, software y comunicaciones. Esto incluye una revisión de los Controladores Lógicos Programables (PLC), la estación centralizada de Interfaz Hombre-Máquina (HMI), así como la red de comunicación, con un énfasis en la seguridad y la conformidad con las mejores prácticas. El objetivo de esta auditoría es garantizar la protección de la infraestructura crítica y la continuidad de las operaciones de generación de energía de EnerCorp en un entorno de crecientes amenazas cibernéticas y desafíos de seguridad. (para más detalle ver Anexo 2).

Estudios previos: Estudios previos: La revisión de documentación es un paso fundamental en el proceso de auditoría de seguridad del sistema SCADA de EnerCorp. Este proceso implica la evaluación de todos los documentos relacionados con el sistema, incluyendo, pero no limitándose a, políticas y procedimientos de seguridad. Sin embargo, como se propuso en el caso de estudio, se ha observado que la documentación de seguridad es inexistente, y la seguridad se basa únicamente en los manuales de configuración de los dispositivos y en prácticas básicas descritas en dichos manuales.

Además, se tuvo como base el desarrollo de un mapa de riesgos que proporcionó información relevante sobre los activos, amenazas y vulnerabilidades más propensos en los sistemas industriales SCADA. Estos riesgos afectan a los activos mencionados anteriormente, que son el PLC, HMI y la red, y son los que se evaluarán, proponiendo controles de acuerdo con el marco de ciberseguridad de la NIST.

En conjunto, la revisión de documentación hubiera sido esencial para establecer una base sólida en la auditoría de seguridad, ya que proporciona información clave sobre la infraestructura, las políticas y las experiencias previas. Lamentablemente, la empresa no posee dicha información, lo que resulta en una evaluación inicial, tal como lo muestra el CSF NIST. (para más detalle ver Anexo 2).

- **Asignación del equipo de auditoría**

Selección de auditores: Para llevar a cabo una auditoría de seguridad exitosa en el sistema SCADA de EnerCorp, es esencial seleccionar cuidadosamente a los miembros del equipo de auditoría. El equipo estará compuesto por profesionales altamente calificados y experimentados en el campo de la seguridad de sistemas SCADA. Estos auditores son individuos que han demostrado su competencia en la identificación de riesgos de seguridad, la evaluación de controles y la aplicación de estándares de buenas prácticas internacionales. (para más detalle ver Anexo 2).

Competencias requeridas: Los auditores designados deben poseer un conjunto diverso de competencias técnicas y habilidades especializadas. Se requerirá que demuestren profundo conocimiento en seguridad informática, lo que abarca desde la comprensión de las vulnerabilidades y amenazas cibernéticas hasta la aplicación de contramedidas efectivas. Además, deberán aportar una sólida experiencia en auditoría de sistemas industriales, con un enfoque en la evaluación de la seguridad de sistemas SCADA en entornos industriales y críticos.

Un aspecto clave es que los auditores también deben estar familiarizados con el marco de ciberseguridad del CSF NIST, ya que este marco es una referencia importante para evaluar y mejorar la seguridad en sistemas SCADA. La competencia en el CSF NIST les permitirá aplicar un enfoque sólido y basado en estándares a la auditoría, asegurando que se cumplan las mejores prácticas internacionales y que se propongan soluciones efectivas para abordar las vulnerabilidades identificadas.

La selección cuidadosa y la formación de este equipo de auditores garantizarán que la auditoría se lleve a cabo de manera completa y precisa, y que se puedan identificar, evaluar y mitigar los riesgos de seguridad en el sistema SCADA de EnerCorp de manera efectiva. (para más detalle ver Anexo 2).

- **Reunión inicial**

Participantes: La reunión inicial convocará a una variedad de partes interesadas clave para asegurar una visión completa y coordinada del proceso de auditoría. Esto incluye a los miembros del equipo de auditoría, expertos en seguridad de sistemas SCADA, representantes del departamento de Tecnologías de la Información (TI) de EnerCorp, quienes son responsables de la infraestructura de TI, y los responsables del sistema SCADA, que están familiarizados con las operaciones y el funcionamiento del sistema.

Objetivos de la reunión: La reunión inicial tiene varios objetivos cruciales. En primer lugar, se busca establecer una comunicación clara y fluida entre todos los participantes, promoviendo un entorno colaborativo y de confianza. Además, la reunión tiene como objetivo alinear las expectativas de todas las partes involucradas, asegurando que todos tengan una comprensión clara de lo que se espera del proceso de auditoría. También se revisará y confirmará el alcance de la auditoría, garantizando que no quede lugar a ambigüedades ni omisiones. Por último, se acordará un cronograma de trabajo que defina las etapas, los plazos y las responsabilidades de cada parte, lo que permitirá una ejecución eficiente del proceso de auditoría.

Temas para tratar: Durante la reunión, se abordarán diversos temas cruciales. Entre ellos, se discutirán en detalle los objetivos de la auditoría, que incluyen la identificación de riesgos y vulnerabilidades, y la evaluación de controles de seguridad. Se considerarán los riesgos conocidos, como amenazas cibernéticas anteriores o riesgos de seguridad que puedan haber afectado al sistema SCADA de EnerCorp. La disponibilidad de documentación relevante, como políticas de seguridad y registros de configuración, será evaluada para garantizar que esté completa y sea accesible. Se acordarán los accesos necesarios al sistema SCADA para los auditores, garantizando que puedan llevar a cabo evaluaciones efectivas sin interrupciones. Además, se discutirán los requisitos logísticos, como horarios, ubicaciones y recursos necesarios para la auditoría.

En resumen, la reunión inicial establecerá las bases sólidas para un proceso de auditoría de seguridad exitoso y bien coordinado. Asegurará que todas las partes involucradas estén alineadas en cuanto a objetivos y expectativas, lo que es esencial para llevar a cabo una evaluación integral y efectiva del sistema SCADA de EnerCorp.

3.4.4 Ejecución de la Auditoría de Seguridad en Sistemas Industriales SCADA

- **Evaluación de riesgos y controles**

Realización de entrevistas: Se realizarán entrevistas con los principales empleados y responsables del sistema SCADA de EnerCorp para obtener una descripción más detallada del entorno operativo y la seguridad del sistema SCADA de la empresa. Para comprender completamente cómo se utilizan los sistemas en las operaciones diarias, identificar los procesos críticos, comprender las políticas y procedimientos en uso y conocer las preocupaciones de seguridad expresadas por los empleados, serán necesarias estas entrevistas. Además, se llevarán a cabo investigaciones sobre las percepciones y experiencias del personal sobre los riesgos de seguridad. Los auditores podrán obtener una visión

contextual y útil del sistema SCADA a través de esta interacción con el personal. (Consulte Anexo 2 para obtener más información.)

Análisis de documentación: En esta fase, se revisarán todos los documentos relacionados con la seguridad y la operación del sistema SCADA. Esto incluirá políticas de seguridad, procedimientos, registros de riesgos previos, diagramas de red, informes de auditoría anteriores y cualquier otra documentación relevante. El objetivo de este análisis es evaluar la efectividad de los controles implementados en el sistema SCADA de EnerCorp. Se verificará si las políticas y procedimientos existentes se alinean con las mejores prácticas y estándares de seguridad internacionales, como el CSF NIST. Además, se buscarán evidencias de riesgos previos o debilidades de seguridad que requieran atención durante la auditoría.

En conjunto, la realización de entrevistas y el análisis de documentación permitirán a los auditores reunir una amplia gama de información, tanto cualitativa como cuantitativa. Esta información será esencial para la identificación de riesgos y vulnerabilidades específicos, así como para la evaluación de los controles existentes. El resultado de esta etapa sentará las bases para las acciones de auditoría subsiguientes, incluyendo la formulación de recomendaciones de mejora y la validación de la seguridad del sistema SCADA de EnerCorp. (para más detalle ver los Anexos B).

- **Ejecución de procedimientos checklist basado en la CSF NIST**

Utilización de la lista de verificación: En esta fase inicial, se empleó lista de verificación que se sustenta en los principios y estándares de seguridad definidos por el Framework de Ciberseguridad del NIST. Esta lista de verificación es una herramienta esencial para orientar la auditoría de seguridad. Proporciona una guía estructurada que garantiza que ningún control de seguridad relevante pase desapercibido. Cada elemento de la lista de verificación se alinea con los marcos y directrices establecidos por el NIST, lo que asegura una cobertura completa y detallada de todos los aspectos esenciales de la seguridad.

Revisión de controles: La revisión minuciosa de los controles de seguridad es el núcleo de la auditoría. En esta etapa, se analiza la implementación y la eficacia de una variedad de controles críticos diseñados para proteger la infraestructura y los activos de una organización. Estos controles abarcan una amplia gama de áreas, desde la autenticación y el acceso físico y lógico, hasta la gestión de cambios, la monitorización de eventos y la resiliencia, incluida la capacidad de recuperación ante desastres. La auditoría evalúa cómo se aplican estos controles en la práctica, si se siguen de manera consistente y si logran los resultados deseados en términos de seguridad y protección de datos.

Para la evaluación apropiada de los niveles de madurez para cada uno de los controles se establecieron cuatro preguntas, cada una con 5 posibles respuestas:

- Definición de la política: Sin política, Política no oficial, Política parcialmente documentada, Política documentada, Política oficialmente aprobada.
- Implementación del Control: No se ha implementado, Fragmento de la política implementadas, Implementado en ciertos sistemas, Implementado en la mayoría de los sistemas, Implementado en la totalidad de los sistemas.

- Automatización del Control: No automatizado, Fragmento de la política automatizadas, Automatizado en ciertos sistemas, Automatizado en la mayoría de los sistemas, Automatizado en la totalidad de los sistemas.
- Informe del control a la alta dirección: No reportado, Fragmento de la política informadas, Informado en ciertos sistemas, Reportado en la mayoría de los sistemas, Reportado en la totalidad de los sistemas.

La categorización de los niveles de madurez se estableció de la siguiente manera:

- Nivel uno: Hay políticas aprobadas para la totalidad de controles.
- Nivel dos: La totalidad de controles están implementados.
- Nivel tres: La totalidad de controles están automatizados.
- Nivel cuatro: La totalidad de controles están informados y reportados.

(para más detalle ver los Anexos 2).

- **Documentación de observaciones y hallazgos:**

Registro detallado de hallazgos: Después de completar la lista de verificación basada en el Framework del NIST, para ello, se procedió a documentar cualquier hallazgo que revele inconformidades con los estándares y controles de seguridad establecidos. Cada hallazgo se registrará de manera detallada, incluyendo una descripción precisa del problema, su ubicación en el sistema SCADA y cualquier contexto relevante. Además, se asignará un nivel de gravedad o prioridad a cada inconformidad para ayudar en la posterior gestión de correcciones. (para más detalle ver el Anexo 2).

- **Elaboración del informe de auditoría**

Estructura del informe: El informe de auditoría está diseñado para ser un documento claro y organizado que brinde a los interesados una visión completa de la auditoría. La estructura típica del informe incluye:

Descripción del alcance de la auditoría: En esta sección, se estableció qué aspectos del sistema SCADA se evaluaron y qué no se incluyó en la auditoría. Esto ayuda a los lectores a comprender las limitaciones de la auditoría.

Métodos utilizados Se caracterizó los métodos y enfoques que se aplicaron durante la auditoría, lo que incluye la lista de verificación basada en el Framework del NIST, las entrevistas, la revisión de documentación y cualquier herramienta o técnica especializada utilizada.

Hallazgos clave: Esta sección es crucial y resume de manera concisa los hallazgos más significativos de la auditoría. Aquí se destacan las inconformidades, vulnerabilidades y riesgos identificados, junto con una descripción de su gravedad y sus posibles consecuencias.

Recomendaciones de mejora: Las recomendaciones se presentan en el informe para abordar los hallazgos identificados. Cada recomendación debe ser específica, accionable y respaldada por una justificación sólida. Además, se pueden incluir recomendaciones sobre políticas, procedimientos, tecnologías, capacitación y otros aspectos relevantes de la seguridad. (para más detalle ver los Anexo 3).

3.4.5 Resultado de la Auditoría de Seguridad en Sistemas Industriales SCADA

- **Presentación del informe a la dirección**

Reunión con la alta dirección: Organizar una reunión con la alta dirección de EnerCorp es esencial para comunicar de manera efectiva los resultados de la auditoría. Durante esta reunión, se proporciona un resumen detallado de los hallazgos clave, las inconformidades identificadas y las recomendaciones de mejora. Esta reunión no solo permite una interacción directa con los líderes de la organización, sino que también brinda la oportunidad de aclarar dudas y discutir posibles acciones correctivas.

- **Definición de la acción correctiva**

Colaboración con EnerCorp: En este momento, se fomentó a los responsables del sistema SCADA y a otros miembros de EnerCorp a trabajar juntos de manera estrecha. Para garantizar que las acciones correctivas se adapten a las necesidades y desafíos específicos de la organización, es esencial este enfoque colaborativo. Al trabajar juntos, los auditores y el personal interno de EnerCorp pueden garantizar que las soluciones propuestas sean viables y se ajusten a la cultura y los objetivos comerciales de la empresa, lo que garantiza una implementación efectiva y sostenible.

- **Seguimiento de las acciones correctivas**

Monitoreo continuo: El monitoreo continuo es una práctica esencial en el seguimiento de las acciones correctivas. Implica la observación constante y la supervisión de la implementación de las acciones correctivas para asegurarse de que se estén llevando a cabo de acuerdo con lo planeado. Esto puede incluir la revisión de registros, el análisis de métricas de seguridad y la verificación de que los procedimientos actualizados se estén siguiendo de manera efectiva.

4. Conclusiones y recomendaciones

4.1 Conclusiones

El mapa de riesgos creado mediante el análisis completo de vulnerabilidades y amenazas facilita a los expertos en seguridad de los sistemas SCADA la identificación de diversos riesgos presentes en entornos industriales. Este proceso ayuda a comprender mejor el nivel de exposición a riesgos de estos sistemas, lo que es esencial para crear planes de seguridad y estrategias de mitigación.

De esta manera se logró identificar los lineamientos más sólidos para llevar a cabo auditorías de seguridad en los sistemas SCADA al revisar y analizar las normas, estándares y buenas prácticas internacionales en seguridad de estos sistemas. Este proceso permitió la creación de un modelo de ejecución de auditorías que se ajusta a las mejores prácticas globales y está especialmente adaptado para entornos industriales.

El modelo de auditoría de ejecución está diseñado para evaluar el plan de controles de este proyecto y tiene como objetivo reducir los diversos riesgos que se encuentran en el mapa de riesgos de los sistemas SCADA. Este modelo, que se basa en las mejores prácticas

internacionales en seguridad informática, permite a los expertos en seguridad de los sistemas SCADA realizar auditorías de manera eficiente y efectiva, lo que reduce los riesgos y garantiza la continuidad del negocio.

La validación del modelo de seguridad para la ejecución de auditorías en sistemas SCADA permitió que el método sugerido, que se basa en las mejores prácticas internacionales y en un plan de controles diseñado específicamente para entornos industriales, fuera efectivo. Los resultados de la validación demostraron que el modelo funciona bien para realizar auditorías de seguridad en sistemas industriales, lo que permite a las empresas identificar riesgos y vulnerabilidades y aplicar controles efectivos para reducirlos.

Finalmente, con la realización de este trabajo se logró desarrollar un modelo de ejecución de auditorías en sistemas industriales SCADA que se basa en la identificación y el análisis de riesgos, la aplicación de las mejores prácticas internacionales en seguridad informática y un plan de controles adaptado a entornos industriales específicos. Este método permitió a los expertos en seguridad de los sistemas SCADA realizar auditorías de manera eficiente y efectiva, identificando y controlando los riesgos técnicos y sus posibles efectos. Además, el modelo cumple con los estándares y lineamientos más rigurosos en seguridad informática al seguir las mejores prácticas internacionales, lo que aumenta la confiabilidad y la eficacia en la ejecución de auditorías de seguridad en sistemas industriales SCADA.

4.2 Recomendaciones futuras

Para trabajos posteriores, sería beneficioso evaluar la efectividad del modelo implementado mediante un seguimiento y evaluación sistemático en entornos comerciales reales. Con esta estrategia, se podrían obtener datos empíricos sobre cómo funciona el modelo y se podrían obtener comentarios directos de los profesionales involucrados. Comparar los resultados con otros métodos existentes también sería útil para destacar claramente las ventajas y el valor agregado del modelo.

La incorporación de herramientas de automatización y análisis en el proceso de auditoría de seguridad es una recomendación importante. Identificar patrones, detectar anomalías y agilizar el proceso de evaluación de seguridad puede requerir el uso de tecnologías avanzadas como la inteligencia artificial, el aprendizaje automático y el análisis de big data. Además, es esencial llevar a cabo un análisis de costo-beneficio para investigaciones futuras. Para ello se requiere un analisis de sensibilidad tanto de los costos como de los beneficios de implementar el modelo de auditoría sugerido. De esta manera al evaluar distintos escenarios donde la viabilidad y el retorno de inversión de implementar el modelo comparándolo con otras opciones disponibles. Este enfoque completo garantizaría que el modelo sea efectivo y valioso a largo plazo.

En el desarrollo de investigaciones futuras, se sugiere profundizar en el análisis de riesgos para SCI y SCADA, tomando en cuenta estándares específicos para estos entornos. Si bien los marcos de referencia generales como COSO, COBIT, ITIL, ISO/IEC 27001 y el Marco de Ciberseguridad de NIST (CSF) proporcionan una base sólida, es importante considerar estándares más enfocados en la seguridad de los SCI y SCADA.

Incorporación de Estándares Relevantes:

Se recomienda incorporar el análisis de los siguientes estándares en investigaciones futuras:

1. ISA/IEC 62443 (Serie de Normas de Seguridad Cibernética para Automatización Industrial): Esta serie proporciona un marco integral para la seguridad de la información y la gestión de riesgos en entornos de automatización industrial.

2. NIST SP 800-82 Rev. 2 (Guía para la Seguridad de SCADA y Sistemas de Control Industrial): Esta guía ofrece recomendaciones prácticas para implementar medidas de seguridad en sistemas SCADA y SCI.

3. CIS Critical Security Controls (CSC): Estos controles identifican las vulnerabilidades más comunes que afectan los sistemas de información y proporcionan recomendaciones para mitigarlas. Si bien no están específicamente diseñados para SCI y SCADA, muchos de los controles son relevantes para estos entornos.

4. ENISA Good Practice Guide on Industrial Control Systems Security: Esta guía publicada por la Agencia de Ciberseguridad de la Unión Europea (ENISA) ofrece recomendaciones prácticas para la seguridad de los SCI y SCADA en Europa.

5. CNERI (Centro Nacional para la Protección de las Infraestructuras Críticas y la Ciberseguridad) - Guías de Seguridad para Infraestructuras Críticas: Estas guías, publicadas por el CNERI en España, proporcionan recomendaciones específicas para la seguridad de las infraestructuras críticas, incluyendo los SCI y SCADA.

6. IEC 61511 (Seguridad Funcional de los Sistemas Instrumentados de Seguridad): Esta norma internacional define los requisitos para la seguridad funcional de los sistemas instrumentados de seguridad (SIS), que son componentes críticos para la seguridad en la industria de procesos.

7. IEC 61850 (Comunicaciones para Sistemas de Automatización de Subestaciones de Energía): Esta norma internacional define un protocolo de comunicación estándar para subestaciones eléctricas, que son componentes esenciales en la red eléctrica.

La consideración de estos estándares específicos permitirá un análisis de riesgos más completo y preciso para SCI y SCADA, orientado a la identificación y mitigación de las amenazas y vulnerabilidades más relevantes en estos entornos.

Investigación en Áreas Específicas:

Además de incorporar estándares específicos, se sugieren las siguientes áreas de investigación futura:

- Análisis de amenazas y vulnerabilidades emergentes en SCI y SCADA: Mantenerse actualizado sobre las nuevas amenazas y vulnerabilidades es crucial para la gestión efectiva de riesgos.

- Desarrollo de metodologías adaptadas para la evaluación de riesgos en SCI y SCADA: Las metodologías existentes pueden necesitar ajustes para adaptarse a las características específicas de los SCI y SCADA.
- Implementación de soluciones de seguridad personalizadas para SCI y SCADA: Las soluciones de seguridad genéricas pueden no ser adecuadas para los entornos complejos de SCI y SCADA.
- Evaluación de la eficacia de las medidas de seguridad en SCI y SCADA: Es importante medir y evaluar el impacto de las medidas de seguridad implementadas.
- Promoción de la concienciación sobre la seguridad en SCI y SCADA: La capacitación y concienciación del personal son esenciales para una cultura de seguridad efectiva.

Al enfocarse en estas áreas de investigación, se puede contribuir a un mejor conocimiento y comprensión de los riesgos en SCI y SCADA, lo que permitirá a las organizaciones proteger sus activos críticos de manera más efectiva.

Anexos

Anexo 1:

Tabla 40.

Mapa de Riesgos

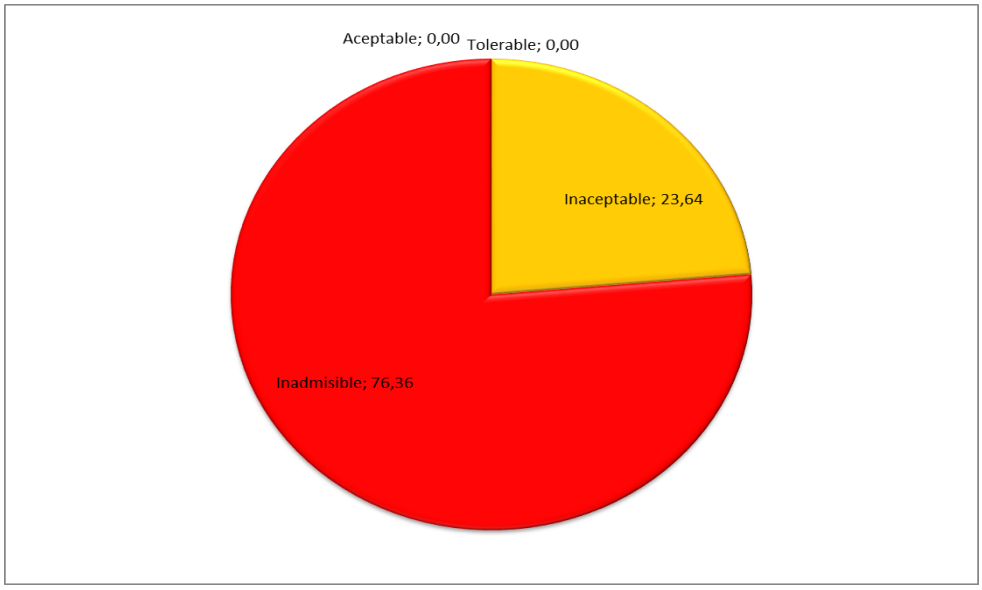
Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5				(47) -	(11) - (13) - (14) -
Probable	4				(6) - (9) - (10) - (12) - (16) - (17) - (18) - (19) - (20) - (21) - (22) - (24) -	(29) - (45) - (46) -
Posible	3			(4) - (7) - (8) - (15) - (23) - (31) - (32) - (36) - (39) -	(1) - (2) - (3) - (5) -	
Improbable	2					
Raro	1					

DISTRIBUCIÒN PORCENTUAL		
ZONA	%	Total riesgos
Aceptable	0,00	0
Tolerable	0,00	0
Inaceptable	23,64	13
Inadmisible	76,36	42

Nota. Esta matriz se utiliza para evaluar y visualizar el nivel de riesgo de diferentes eventos o situaciones, ayudando a priorizar acciones de mitigación.

Figura 19.

Rango de riesgo



Nota. Este gráfico representa la distribución de datos en cuatro categorías, indicando que una mayoría significativa cae bajo la categoría ‘Inadmisible’.

Anexo 2: Auditoria

Tabla 41.

Planeación

LOGO	AUDITORIA INTERNA	FORMATO No.
PROCESO: CONTROL DE SCADA	VERSION	###

Fecha de elaboración del Plan						FECHA DE EJECUCION						AUDITORIA
DD		MM		AA		DESDE			HASTA			###
						DD	MM	AA	DD	MM	AA	

Objetivo de la auditoria:	Identificar y evaluar los controles de tecnología que aseguran la confidencialidad, integridad y disponibilidad
Alcance:	La evaluación de los controles generales de tecnología se va realizar enmarcada en las mejores prácticas de la Norma marco de ciberseguridad de la NIST (CSF NIST) teniendo en cuenta los numerales: PR.AC-1: Identidades y credenciales: PR.AC-2: Acceso físico a activos: PR.AC-3: Acceso remoto: PR.AC-4: Permisos y autorizaciones: PR.AC-5: Integridad de la red: PR.AC-7: Autenticación de usuarios: PR.AT-1: Usuarios informados y capacitados: PR.DS-6: Mecanismos de comprobación de integridad: PR.IP-3: Control de cambio de configuración: PR.IP-4: Copias de seguridad de la información: PR.IP-9: Planes de respuesta y recuperación: PR.PT-1: Registros de auditoría o archivos: PR.PT-2: Medios extraíbles protegidos: PR.PT-4: Protección de redes de comunicaciones y control: DE.CM-1: Monitoreo de red para eventos de seguridad: DE.CM-2: Monitoreo del entorno físico: DE.CM-3: Monitoreo de actividad del personal: DE.CM-4: Detección de código malicioso: DE.CM-7: Monitoreo de personal, conexiones y dispositivos no autorizados: DE.CM-8: Escaneos de vulnerabilidades:

Equipo auditor y acompañantes

Ítem	Nombres y Apellidos	Papel que desempeña
1	RONY CAICEDO	AUDITOR
2		
3		
4		
5		
6		

Documentos de Referencia (Estudio previos)

Manual no oficial de Seguridad de la información y Ciberseguridad. Procedimiento no oficial de Políticas de Seguridad de la Información y Ciberseguridad.	Mapa de riesgos determinado en el punto 3.1.3

Agenda de la auditoría						
Ítem	Proceso	Procedimientos y/o temas	FECHA			HORA
			DD	MM	AA	

Líder de Auditoría:		**Equipo Auditor:**	
Fecha de inicio auditoría:		**Fecha de Fin auditoria:**	
Area auditada:		**Proceso auditado:**	
Lugar:		**Periodo evaluado:**	
Población:		**Muestra:**	
Tipo de Auditoria: **(1 Parte / 2 Parte / 3 Parte)**		**Método de Auditoría (Ubicación):** **Remoto / En sitio**	
Elaborado por:		**Aprobado Por:**	
Fecha Elaboración:		**Fecha Aprobación:**	

Nota. Este documento es utilizado para planificar y ejecutar auditorías internas, asegurando que se cumplan los estándares y controles establecidos.

Ejecución

La ejecución se hará en las siguientes ventanas procurando tener la mejor comprensión de la empresa

1 Mapa de Riesgo	Informacion que para este trabajo se adquirio del punto del mapa de riesgo

2 Validar controles	Controles propuestos para especificamente para la seguridad de un sistema SCADA

3 cumplimiento del CSF NIST	Nivel de madurez dependiendo de la validacion de las expecttivas según el nivel de aseguramiento de los dispositivos

Tabla 42.

Mapa de riesgos

Activo	Amenaza	Riesgo
PLC	Phishing	(1) -Posibilidad que la amenaza: Phishing, afecte el activo: PLC
	Malware	(9) -Posibilidad que la amenaza: Malware, afecte el activo: PLC
	DoS	(17) -Posibilidad que la amenaza: DoS, afecte el activo: PLC
	Buffer overflow	(25) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: PLC
	Inyección de código	(33) -Posibilidad que la amenaza: Inyección de código, afecte el activo: PLC
	Acceso no autorizado	(41) -Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: PLC
	Fallos humanos	(49) -Posibilidad que la amenaza: Fallos humanos, afecte el activo: PLC
HMI	Phishing	(4) -Posibilidad que la amenaza: Phishing, afecte el activo: EQUIPAMENTO PANTALLA HMI
	Malware	(12) -Posibilidad que la amenaza: Malware, afecte el activo: EQUIPAMENTO PANTALLA HMI
	DoS	(20) -Posibilidad que la amenaza: DoS, afecte el activo: EQUIPAMENTO PANTALLA HMI
	Buffer overflow	(28) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: EQUIPAMENTO PANTALLA HMI
	Inyección de código	(36) -Posibilidad que la amenaza: Inyección de código, afecte el activo: EQUIPAMENTO PANTALLA HMI
	Acceso no autorizado	(44) -Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: EQUIPAMENTO PANTALLA HMI
	Fallos humanos	(52) -Posibilidad que la amenaza: Fallos humanos, afecte el activo: EQUIPAMENTO PANTALLA HMI

Nota. Para el activo PLC y la amenaza de Phishing, el riesgo es la posibilidad de que el atacante obtenga información del PLC. Cada celda de la tabla tiene un fondo de color rojo o verde, indicando el nivel de riesgo asociado.

Tabla 43.

Controles

Posibilidad que la amenaza Phishing afecte el activo PLC:
Control: Implementar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access)
Referencia Informativa: CSF Subcategoría PR.PT-4

Posibilidad que la amenaza Malware afecte el activo PLC:
Control: Utilizar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access)
Referencia Informativa: CSF Subcategoría PR.PT-4

Posibilidad que la amenaza DoS afecte el activo PLC:
Control: Implementar medidas para garantizar la disponibilidad y el rendimiento de los sistemas PLC incluso durante un ataque de Denegación de Servicio (DoS).
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra accesos no autorizados (Protect against Unauthorized Access)
Referencia Informativa: CSF Subcategoría PR.PT-1

Posibilidad que la amenaza Buffer Overflow afecte el activo PLC:
Control: Implementar medidas para evitar la ejecución no autorizada de código en el sistema, incluida la validación de firmas digitales para el software crítico.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra ejecución no autorizada de código (Protect against Unauthorized Execution of Code)
Referencia Informativa: CSF Subcategoría PR.PT-2

Posibilidad que la amenaza Inyección de Código afecte el activo PLC:
Control: Implementar medidas para validar y sanitizar la entrada de datos para prevenir la inyección de código malicioso.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra ejecución no autorizada de código (Protect against Unauthorized Execution of Code)
Referencia Informativa: CSF Subcategoría PR.PT-3

Posibilidad que la amenaza Acceso no Autorizado afecte el activo PLC:
Control: Aplicar controles de acceso rigurosos, incluida la autenticación de múltiples factores, para limitar el acceso a los sistemas PLC.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access)
Referencia Informativa: Varias subcategorías en la función Protect pueden ser relevantes.

Posibilidad que la amenaza Fallos Humanos afecte el activo PLC:
Control: Implementar controles de acceso basados en roles y proporcionar capacitación y concientización regular para reducir la probabilidad de errores humanos.
Función CSF: Proteger (Protect) y Detectar (Detect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access) y Detectar la ocurrencia de eventos de seguridad (Detect)
Referencia Informativa: CSF Subcategorías PR.AC-3 y DE.CM-8

Posibilidad que la amenaza Phishing afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Implementar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access)
Referencia Informativa: CSF Subcategoría PR.PT-4

Posibilidad que la amenaza Malware afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Utilizar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access)
Referencia Informativa: CSF Subcategoría PR.PT-4

Posibilidad que la amenaza DoS afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Implementar medidas para garantizar la disponibilidad y el rendimiento de los sistemas HMI incluso durante un ataque de Denegación de Servicio (DoS).
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra accesos no autorizados (Protect against Unauthorized Access)
Referencia Informativa: CSF Subcategoría PR.PT-1

Posibilidad que la amenaza Buffer Overflow afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Implementar medidas para evitar la ejecución no autorizada de código en el sistema, incluida la validación de firmas digitales para el software crítico.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra ejecución no autorizada de código (Protect against Unauthorized Execution of Code)
Referencia Informativa: CSF Subcategoría PR.PT-2

Posibilidad que la amenaza Inyección de Código afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Implementar medidas para validar y sanitizar la entrada de datos para prevenir la inyección de código malicioso.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra ejecución no autorizada de código (Protect against Unauthorized Execution of Code)
Referencia Informativa: CSF Subcategoría PR.PT-3

Posibilidad que la amenaza Acceso no Autorizado afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Aplicar controles de acceso rigurosos, incluida la autenticación de múltiples factores, para limitar el acceso a los sistemas HMI.
Función CSF: Proteger (Protect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access)
Referencia Informativa: Varias subcategorías en la función Protect pueden ser relevantes.

Posibilidad que la amenaza Fallos Humanos afecte el activo EQUIPAMENTO PANTALLA HMI:
Control: Implementar controles de acceso basados en roles y proporcionar capacitación y concientización regular para reducir la probabilidad de errores humanos.
Función CSF: Proteger (Protect) y Detectar (Detect)
Categoría y Subcategoría: Proteger contra acceso no autorizado (Protect against Unauthorized Access) y Detectar la ocurrencia de eventos de seguridad (Detect)
Referencia Informativa: CSF Subcategorías PR.AC-3 y DE.CM-8

PR.AC-1: Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.

PR.AC-2: Se gestiona y se protege el acceso físico a los activos.

PR.AC-3: Se gestiona el acceso remoto.

PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.

PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).

PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o multiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).

PR.AT-1: Todos los usuarios están informados y capacitados.

PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.

PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.

PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.

PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).

PR.PT-1: Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.

PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.

PR.PT-4: Las redes de comunicaciones y control están protegidas.

DE.CM-1: Se monitorea la red para detectar posibles eventos de seguridad cibernética.

DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.

DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.

DE.CM-4: Se detecta el código malicioso.

DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.

DE.CM-8: Se realizan escaneos de vulnerabilidades.

Nota. La tabla y secuencia anterior muestran los pasos a tener en cuenta para el control de riesgos

Tabla 44.

Entrevista

NOMBRE_EMPRESA			
Nombre de la Auditoria:			
Nombre del Auditor Lider:			
Trabajo realizado por el auditor:			
Fecha de la Entrevista:			
Hora Inicio: Hora Fin:			
Entrevistados (Nombre completo / Cargo):			
Area Entrevistada:			
Objetivo de la Auditoria:			
Alcance de la Auditoria:			
Criterios de la Auditoria:			
Método de la Auditoria:			
Conclusiones Generales:			

Nota. Hoja de registro para documentar las horas de trabajo incluyendo los tiempos de inicio y fin, las horas totales trabajadas, de auditoria.

Tabla 45.

Información consultar auditoria

Información a consultar	Documentos y/o registros	Conformidad / No Conformidad	Comentarios / observaciones / conclusiones
PR.AC-1: Identidades y credenciales:			
¿La política para emitir, administrar, verificar, revocar y auditar identidades y credenciales está oficialmente aprobada?		No Conformidad	NO
¿Se ha implementado en la totalidad de los sistemas el control para gestionar identidades y credenciales?		No Conformidad	NO
¿Está completamente automatizado el proceso de gestión de identidades y credenciales?		No Conformidad	NO
PR.AC-2: Acceso físico a activos:			
¿Existe una política oficialmente aprobada para gestionar y proteger el acceso físico a los activos?		No Conformidad	NO
¿Se ha implementado en la totalidad de los sistemas el control para proteger el acceso físico a los activos?		No Conformidad	NO
¿Está completamente automatizado el control para gestionar el acceso físico?		No Conformidad	NO
PR.AC-3: Acceso remoto:			
¿Existe una política oficialmente aprobada para gestionar el acceso remoto?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para gestionar el acceso remoto?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para el acceso remoto?		No Conformidad	NO
PR.AC-4: Permisos y autorizaciones:			
¿La política documentada gestiona de manera efectiva los permisos y autorizaciones de acceso?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para gestionar permisos y autorizaciones?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para permisos y autorizaciones?		No Conformidad	NO
PR.AC-5: Integridad de la red:			
¿La política documentada protege de manera efectiva la integridad de la red?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para proteger la integridad de la red?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para la integridad de la red?		No Conformidad	NO
PR.AC-7: Autenticación de usuarios:			
¿Existe una política oficialmente aprobada para autenticar usuarios, dispositivos y otros activos?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para autenticar usuarios, dispositivos y activos?		No Conformidad	NO
¿Está completamente automatizado el control para la autenticación?		No Conformidad	NO
PR.AT-1: Usuarios informados y capacitados:			
¿Existe una política oficialmente aprobada para informar y capacitar a todos los usuarios?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para informar y capacitar a los usuarios?		No Conformidad	NO
¿Está completamente automatizado el control para la información y capacitación de usuarios?		No Conformidad	NO
PR.DS-6: Mecanismos de comprobación de integridad:			
¿Se han establecido procesos de control de cambio de configuración según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para verificar la integridad de software, firmware e información?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para comprobar la integridad?		No Conformidad	NO
PR.IP-3: Control de cambio de configuración:			
¿Existen procesos de control de cambio de configuración establecidos?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para el cambio de configuración?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para el cambio de configuración?		No Conformidad	NO
PR.IP-4: Copias de seguridad de la información:			
¿Se realizan, mantienen y prueban copias de seguridad de la información según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para las copias de seguridad de la información?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para las copias de seguridad?		No Conformidad	NO

PR.IP-9: Planes de respuesta y recuperación:			
¿Existen planes de respuesta a incidentes y continuidad del negocio gestionados según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para gestionar planes de respuesta y recuperación?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para la gestión de planes de respuesta y recuperación?		No Conformidad	NO
PR.PT-1: Registros de auditoría o archivos:			
¿Los registros de auditoría o archivos se determinan, documentan e implementan según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para la gestión de registros de auditoría?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para la gestión de registros de auditoría?		No Conformidad	NO
PR.PT-2: Medios extraíbles protegidos:			
¿Se protegen los medios extraíbles y se restringe su uso según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para proteger y gestionar el uso de medios extraíbles?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para proteger medios extraíbles?		No Conformidad	NO
PR.PT-4: Protección de redes de comunicaciones y control:			
¿Las redes de comunicaciones y control están protegidas según la política?		No Conformidad	PARCIAL
¿Se ha implementado en la mayoría de los sistemas el control para proteger las redes de comunicaciones y control?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para proteger redes de comunicaciones y control?		No Conformidad	NO
DE.CM-1: Monitoreo de red para eventos de seguridad:			
¿Se monitorea la red para detectar posibles eventos de seguridad cibernética según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para el monitoreo de eventos de seguridad en la red?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para el monitoreo de eventos de seguridad?		No Conformidad	NO
DE.CM-2: Monitoreo del entorno físico:			
¿Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para el monitoreo del entorno físico?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para el monitoreo del entorno físico?		No Conformidad	NO
DE.CM-3: Monitoreo de actividad del personal:			
¿Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para el monitoreo de la actividad del personal?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para el monitoreo de la actividad del personal?		No Conformidad	NO
DE.CM-4: Detección de código malicioso:			
¿Se detecta el código malicioso según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para la detección de código malicioso?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para la detección de código malicioso?		No Conformidad	NO
DE.CM-7: Monitoreo de personal, conexiones y dispositivos no autorizados:			
¿Se realiza el monitoreo del personal, conexiones y dispositivos no autorizados según la política?		No Conformidad	PARCIAL
¿Se ha implementado en la mayoría de los sistemas el control para el monitoreo de personal, conexiones y dispositivos no autorizados?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para el monitoreo de personal, conexiones y dispositivos no autorizados?		No Conformidad	NO
DE.CM-8: Escaneos de vulnerabilidades:			
¿Se realizan escaneos de vulnerabilidades según la política?		No Conformidad	NO
¿Se ha implementado en la mayoría de los sistemas el control para realizar escaneos de vulnerabilidades?		No Conformidad	NO
¿Está parcial o completamente automatizado el control para realizar escaneos de vulnerabilidades?		No Conformidad	NO

Nota. La tabla muestra una lista de chequeo para determinar la conformidad en la realización de la auditoria.

Cumplimiento del CSF NIST

Nombre de la Auditoria:

Nombre del Auditor Lider:

Trabajo realizado por el auditor:

Tabla 46.

Validación de la madurez de los controles

Funcion	Categoria	controles	Definicion de politica	Control implmentado	Control automatizado	Control informado a la empresa	Valor
PROTEGER PR	PR.AC-1	Identidades y credenciales	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.AC-2	Acceso físico a activos	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.AC-3	Acceso remoto	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.AC-4	Permisos y autorizaciones	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.AC-5	Integridad de la red	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.AC-7	Autenticación de usuarios	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.AT-1	Usuarios informados y capacitados	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.DS-6	Mecanismos de comprobación de integridad	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.IP-3	Control de cambio de configuración	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.IP-4	Copias de seguridad de la información	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.IP-9	Planes de respuesta y recuperación	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.PT-1	Registros de auditoría o archivos	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.PT-2	Medios extraíbles protegidos	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
PROTEGER PR	PR.PT-4	Protección de redes de comunicaciones y control	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
Detectar DE	DE.CM-1	Monitoreo de red para eventos de seguridad	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
Detectar DE	DE.CM-2	Monitoreo del entorno físico	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
Detectar DE	DE.CM-3	Monitoreo de actividad del personal	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
Detectar DE	DE.CM-4	Detección de código malicioso	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
Detectar DE	DE.CM-7	Monitoreo de personal, conexiones y dispositivos no autorizados	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5
Detectar DE	DE.CM-8	Escaneos de vulnerabilidades	Política no oficial	Fragmento de la política implementadas	No automatizado	No reportado	0,5

Area auditada:		Equipo Auditor:	
Lugar:		Fecha de Fin auditoria:	
Auditoria: (1 Parte / 2 Parte		"Método de Auditoría (Ubicación):Remoto / En	
		Proceso auditado:	
		Periodo evaluado:	

Nota. La tabla está codificada por colores en tonos de rosa y púrpura, indicando diferentes categorías o niveles de información. Cada fila representa una función o rol específico, con detalles correspondientes definiendo políticas, controles de acceso y medidas de seguridad.

Tabla 47.

Validación de la madurez de cibersegruidad

Función	Categoría	Subcategoría	Estado actual		Objetivo deseado		Prioridad	
			Logro	Nivel	Logro	Nivel	Brecha	Prioridad
IDENTIFICAR (ID)	**Gestión de activos (ID.AM):** Los datos, el personal, los dispositivos, los sistemas y las instalaciones que permiten a la organización alcanzar los objetivos empresariales se identifican y se administran de forma coherente con su importancia relativa para los objetivos organizativos y la estrategia de riesgos de la organización.	**ID.AM-1:** Los dispositivos y sistemas físicos dentro de la organización están inventariados.	Parcial	1	Adaptable	4	3	Alta
		ID.AM-2: Las plataformas de software y las aplicaciones dentro de la organización están inventariadas.	Parcial	1	Adaptable	4	3	Alta
		ID.AM-3: La comunicación organizacional y los flujos de datos están mapeados.	Parcial	1	Adaptable	4	3	Alta
		ID.AM-4: Los sistemas de información externos están catalogados.	Parcial	1	Adaptable	4	3	Alta
		ID.AM-5: Los recursos (por ejemplo, hardware, dispositivos, datos, tiempo, personal y software) se priorizan en función de su clasificación, criticidad y valor comercial.	Parcial	1	Adaptable	4	3	Alta
		ID.AM-6: Los roles y las responsabilidades de la seguridad cibernética para toda la fuerza de trabajo y terceros interesados (por ejemplo, proveedores, clientes, socios) están establecidas.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "ID-AM: Gestión de activos"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Entorno empresarial (ID.BE): Se entienden y se priorizan la misión, los objetivos, las partes interesadas y las actividades de la organización; esta información se utiliza para informar los roles, responsabilidades y decisiones de gestión de los riesgos de seguridad cibernética.	**ID.BE-1:** Se identifica y se comunica la función de la organización en la cadena de suministro.	Parcial	1	Adaptable	4	3	Alta
		ID.BE-2: Se identifica y se comunica el lugar de la organización en la infraestructura crítica y su sector industrial.	Parcial	1	Adaptable	4	3	Alta
		ID.BE-3: Se establecen y se comunican las prioridades para la misión, los objetivos y las actividades de la organización.	Parcial	1	Adaptable	4	3	Alta
		ID.BE-4: Se establecen las dependencias y funciones fundamentales para la entrega de servicios críticos.	Parcial	1	Adaptable	4	3	Alta
		ID.BE-5: Los requisitos de resiliencia para respaldar la entrega de servicios críticos se establecen para todos los estados operativos (p. ej. bajo coacción o ataque, durante la recuperación y operaciones normales).	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "ID-BE: Entorno empresarial"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Gobernanza (ID.GV): Las políticas, los procedimientos y los procesos para administrar y monitorear los requisitos regulatorios, legales, de riesgo, ambientales y operativos de la organización se comprenden y se informan a la gestión del riesgo de seguridad cibernética.	**ID.GV-1:** Se establece y se comunica la política de seguridad cibernética organizacional.	Parcial	1	Adaptable	4	3	Alta
		ID.GV-2: Los roles y las responsabilidades de seguridad cibernética están coordinados y alineados con roles internos y socios externos.	Parcial	1	Adaptable	4	3	Alta
		ID.GV-3: Se comprenden y se gestionan los requisitos legales y regulatorios con respecto a la seguridad cibernética, incluidas las obligaciones de privacidad y libertades civiles.	Parcial	1	Adaptable	4	3	Alta
		ID.GV-4: Los procesos de gobernanza y gestión de riesgos abordan los riesgos de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "ID-GV: Gobernanza"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Evaluación de riesgos (ID.RA): La organización comprende el riesgo de seguridad cibernética para las operaciones de la organización (incluida la misión, las funciones, la imagen o la reputación), los activos de la organización y las personas.	**ID.RA-1**: Se identifican y se documentan las vulnerabilidades de los activos.	Parcial	1	Adaptable	4	3	Alta
		ID.RA-2: La inteligencia de amenazas cibernéticas se recibe de foros y fuentes de intercambio de información.	Parcial	1	Adaptable	4	3	Alta
		ID.RA-3: Se identifican y se documentan las amenazas, tanto internas como externas.	Parcial	1	Adaptable	4	3	Alta
		ID.RA-4: Se identifican los impactos y las probabilidades del negocio.	Parcial	1	Adaptable	4	3	Alta
		ID.RA-5: Se utilizan las amenazas, las vulnerabilidades, las probabilidades y los impactos para determinar el riesgo.	Parcial	1	Adaptable	4	3	Alta
		ID.RA-6: Se identifican y priorizan las respuestas al riesgo.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "ID-RA: Evaluación de riesgos"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Estrategia de gestión de riesgos (ID.RM): Se establecen las prioridades, restricciones, tolerancias de riesgo y suposiciones de la organización y se usan para respaldar las decisiones de riesgos operacionales.	**ID.RM-1:** Los actores de la organización establecen, gestionan y acuerdan los procesos de gestión de riesgos.	Parcial	1	Adaptable	4	3	Alta
		ID.RM-2: La tolerancia al riesgo organizacional se determina y se expresa claramente.	Parcial	1	Adaptable	4	3	Alta
		ID.RM-3: La determinación de la tolerancia del riesgo de la organización se basa en parte en su rol en la infraestructura crítica y el análisis del riesgo específico del sector.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "ID-RM: Estrategia de gestión de riesgos"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Gestión del riesgo de la cadena de suministro (ID.SC): Las prioridades, limitaciones, tolerancias de riesgo y suposiciones de la organización se establecen y se utilizan para respaldar las decisiones de riesgo asociadas con la gestión del riesgo de la cadena de suministro. La organización ha establecido e implementado los procesos para identificar, evaluar y gestionar los riesgos de la cadena de suministro.	**ID.SC-1:** Los actores de la organización identifican, establecen, evalúan, gestionan y acuerdan los procesos de gestión del riesgo de la cadena de suministro cibernética.	Parcial	1	Adaptable	4	3	Alta
		ID.SC-2: Los proveedores y socios externos de los sistemas de información, componentes y servicios se identifican, se priorizan y se evalúan mediante un proceso de evaluación de riesgos de la cadena de suministro cibernético.	Parcial	1	Adaptable	4	3	Alta
		ID.SC-3: Los contratos con proveedores y socios externos se utilizan para implementar medidas apropiadas diseñadas para cumplir con los objetivos del programa de seguridad cibernética de una organización y el plan de gestión de riesgos de la cadena de suministro cibernético.	Parcial	1	Adaptable	4	3	Alta
		ID.SC-4: Los proveedores y los socios externos se evalúan de forma rutinaria mediante auditorías, resultados de pruebas u otras formas de evaluación para confirmar que cumplen con sus obligaciones contractuales.	Parcial	1	Adaptable	4	3	Alta
		ID.SC-5: Las pruebas y la planificación de respuesta y recuperación se llevan a cabo con proveedores.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "ID-SC: Gestión del riesgo de la cadena de suministro"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**

PROTEGER (PR)	**Gestión de identidad, autenticación y control de acceso (PR.AC):** El acceso a los activos físicos y lógicos y a las instalaciones asociadas está limitado a los usuarios, procesos y dispositivos autorizados, y se administra de forma coherente con el riesgo evaluado de acceso no autorizado a actividades autorizadas y transacciones.	**PR.AC-1:** Las identidades y credenciales se emiten, se administran, se verifican, se revocan y se auditan para los dispositivos, usuarios y procesos autorizados.	Parcial	1	Adaptable	4	3	Alta
		PR.AC-2: Se gestiona y se protege el acceso físico a los activos.	Parcial	1	Adaptable	4	3	Alta
		PR.AC-3: Se gestiona el acceso remoto.	Parcial	1	Adaptable	4	3	Alta
		PR.AC-4: Se gestionan los permisos y autorizaciones de acceso con incorporación de los principios de menor privilegio y separación de funciones.	Parcial	1	Adaptable	4	3	Alta
		PR.AC-5: Se protege la integridad de la red (por ejemplo, segregación de la red, segmentación de la red).	Parcial	1	Adaptable	4	3	Alta
		PR.AC-6: Las identidades son verificadas y vinculadas a credenciales y afirmadas en las interacciones.	Parcial	1	Adaptable	4	3	Alta
		PR.AC-7: Se autentican los usuarios, dispositivos y otros activos (por ejemplo, autenticación de un solo factor o múltiples factores) acorde al riesgo de la transacción (por ejemplo, riesgos de seguridad y privacidad de individuos y otros riesgos para las organizaciones).	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "PR-AC: Gestión de identidad, autenticación y control de acceso"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Concienciación y capacitación (PR.AT): El personal y los socios de la organización reciben educación de concienciación sobre la seguridad cibernética y son capacitados para cumplir con sus deberes y responsabilidades relacionados con la seguridad cibernética, en conformidad con las políticas, los procedimientos y los acuerdos relacionados al campo.	**PR.AT-1:** Todos los usuarios están informados y capacitados.	Parcial	1	Adaptable	4	3	Alta
		PR.AT-2: Los usuarios privilegiados comprenden sus roles y responsabilidades.	Parcial	1	Adaptable	4	3	Alta
		PR.AT-3: Los terceros interesados (por ejemplo, proveedores, clientes, socios) comprenden sus roles y responsabilidades.	Parcial	1	Adaptable	4	3	Alta
		PR.AT-4: Los ejecutivos superiores comprenden sus roles y responsabilidades.	Parcial	1	Adaptable	4	3	Alta
		PR.AT-5: El personal de seguridad física y cibernética comprende sus roles y responsabilidades.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "PR-AT: Concienciación y capacitación"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Seguridad de los datos (PR.DS): La información y los registros (datos) se gestionan en función de la estrategia de riesgo de la organización para proteger la confidencialidad, integridad y disponibilidad de la información.	**PR.DS-1:** Los datos en reposo están protegidos.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-2: Los datos en tránsito están protegidos.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-3: Los activos se gestionan formalmente durante la eliminación, las transferencias y la disposición.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-4: Se mantiene una capacidad adecuada para asegurar la disponibilidad.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-5: Se implementan protecciones contra las filtraciones de datos.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-6: Se utilizan mecanismos de comprobación de la integridad para verificar el software, el firmware y la integridad de la información.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-7: Los entornos de desarrollo y prueba(s) están separados del entorno de producción.	Parcial	1	Adaptable	4	3	Alta
		PR.DS-8: Se utilizan mecanismos de comprobación de la integridad para verificar la integridad del hardware.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "PR-DS: Seguridad de los datos"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Procesos y procedimientos de protección de la información (PR.IP): Se mantienen y se utilizan políticas de seguridad (que abordan el propósito, el alcance, los roles, las responsabilidades, el compromiso de la jefatura y la coordinación entre las entidades de la organización), procesos y procedimientos para gestionar la protección de los sistemas de información y los activos.	**PR.IP-1:** Se crea y se mantiene una configuración de base de los sistemas de control industrial y de tecnología de la información con incorporación de los principios de seguridad (por ejemplo, el concepto de funcionalidad mínima).	Parcial	1	Adaptable	4	3	Alta
		PR.IP-2: Se implementa un ciclo de vida de desarrollo del sistema para gestionar los sistemas.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-3: Se encuentran establecidos procesos de control de cambio de la configuración.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-4: Se realizan, se mantienen y se prueban copias de seguridad de la información.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-5: Se cumplen las regulaciones y la política con respecto al entorno operativo físico para los activos organizativos.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-6: Los datos son eliminados de acuerdo con las políticas.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-7: Se mejoran los procesos de protección.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-8: Se comparte la efectividad de las tecnologías de protección.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-9: Se encuentran establecidos y se gestionan planes de respuesta (Respuesta a Incidentes y Continuidad del Negocio) y planes de recuperación (Recuperación de Incidentes y Recuperación de Desastres).	Parcial	1	Adaptable	4	3	Alta
		PR.IP-10: Se prueban los planes de respuesta y recuperación.	Parcial	1	Adaptable	4	3	Alta
		PR.IP-11: La seguridad cibernética se encuentra incluida en las prácticas de recursos humanos (por ejemplo, desaprovisionamiento, selección del personal).	Parcial	1	Adaptable	4	3	Alta
		PR.IP-12: Se desarrolla y se implementa un plan de gestión de las vulnerabilidades.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "PR-IP: Procesos y procedimientos de protección de la información"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Mantenimiento (PR.MA): El mantenimiento y la reparación de los componentes del sistema de información y del control industrial se realizan de acuerdo con las políticas y los procedimientos.	**PR.MA-1:** El mantenimiento y la reparación de los activos de la organización se realizan y están registrados con herramientas aprobadas y controladas.	Parcial	1	Adaptable	4	3	Alta
		PR.MA-2: El mantenimiento remoto de los activos de la organización se aprueba, se registra y se realiza de manera que evite el acceso no autorizado.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "PR-MA: Procesos y procedimientos de protección de la información"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Tecnología de protección (PR.PT): Las soluciones técnicas de seguridad se gestionan para garantizar la seguridad y la capacidad de recuperación de los sistemas y activos, en consonancia con las políticas, procedimientos y acuerdos relacionados.	**PR.PT-1:** Los registros de auditoría o archivos se determinan, se documentan, se implementan y se revisan en conformidad con la política.	Parcial	1	Adaptable	4	3	Alta
		PR.PT-2: Los medios extraíbles están protegidos y su uso se encuentra restringido de acuerdo con la política.	Parcial	1	Adaptable	4	3	Alta
		PR.PT-3: Se incorpora el principio de menor funcionalidad mediante la configuración de los sistemas para proporcionar solo las capacidades esenciales.	Parcial	1	Adaptable	4	3	Alta
		PR.PT-4: Las redes de comunicaciones y control están protegidas.	Parcial	1	Adaptable	4	3	Alta
		PR.PT-5: Se implementan mecanismos (por ejemplo, a prueba de fallas, equilibrio de carga, cambio en caliente o "hot swap") para lograr los requisitos de resiliencia en situaciones normales y adversas.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "PR-PT: Tecnología de protección"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**

DETECTAR (DE)	**Anomalías y Eventos (DE.AE):** se detecta actividad anómala y se comprende el impacto potencial de los eventos.	**DE.AE-1:** Se establece y se gestiona una base de referencia para operaciones de red y flujos de datos esperados para los usuarios y sistemas.	Parcial	1	Adaptable	4	3	Alta
		DE.AE-2: Se analizan los eventos detectados para comprender los objetivos y métodos de ataque.	Parcial	1	Adaptable	4	3	Alta
		DE.AE-3: Los datos de los eventos se recopilan y se correlacionan de múltiples fuentes y sensores.	Parcial	1	Adaptable	4	3	Alta
		DE.AE-4: Se determina el impacto de los eventos.	Parcial	1	Adaptable	4	3	Alta
		DE.AE-5: Se establecen umbrales de alerta de incidentes.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "DE-AE: Anomalías y Eventos"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Monitoreo Continuo de la Seguridad (DE.CM): El sistema de información y los activos son monitoreados a fin de identificar eventos de seguridad cibernética y verificar la eficacia de las medidas de protección.	**DE.CM-1:** Se monitorea la red para detectar posibles eventos de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-2: Se monitorea el entorno físico para detectar posibles eventos de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-3: Se monitorea la actividad del personal para detectar posibles eventos de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-4: Se detecta el código malicioso.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-5: Se detecta el código móvil no autorizado.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-6: Se monitorea la actividad de los proveedores de servicios externos para detectar posibles eventos de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-7: Se realiza el monitoreo del personal, conexiones, dispositivos y software no autorizados.	Parcial	1	Adaptable	4	3	Alta
		DE.CM-8: Se realizan escaneos de vulnerabilidades.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "DE-CM: Monitoreo Continuo de la Seguridad"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Procesos de Detección (DE.DP): Se mantienen y se aprueban los procesos y procedimientos de detección para garantizar el conocimiento de los eventos anómalos.	**DE.DP-1:** Los roles y los deberes de detección están bien definidos para asegurar la responsabilidad.	Parcial	1	Adaptable	4	3	Alta
		DE.DP-2: Las actividades de detección cumplen con todos los requisitos aplicables.	Parcial	1	Adaptable	4	3	Alta
		DE.DP-3: Se prueban los procesos de detección.	Parcial	1	Adaptable	4	3	Alta
		DE.DP-4: Se comunica la información de la detección de eventos.	Parcial	1	Adaptable	4	3	Alta
		DE.DP-5: los procesos de detección se mejoran continuamente.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "DE-DP: Procesos de Detección"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
RESPONDER (RS)	**Planificación de la Respuesta (RS.RP):** Los procesos y procedimientos de respuesta se ejecutan y se mantienen a fin de garantizar la respuesta a los incidentes de seguridad cibernética detectados.	**RS.RP-1:** El plan de respuesta se ejecuta durante o después de un incidente.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RS-RP: Planificación de la Respuesta"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Comunicaciones (RS.CO): Las actividades de respuesta se coordinan con las partes interesadas internas y externas (por ejemplo, el apoyo externo de organismos encargados de hacer cumplir la ley).	**RS.CO-1:** El personal conoce sus roles y el orden de las operaciones cuando se necesita una respuesta.	Parcial	1	Adaptable	4	3	Alta
		RS.CO-2: Los incidentes se informan de acuerdo con los criterios establecidos.	Parcial	1	Adaptable	4	3	Alta
		RS.CO-3: La información se comparte de acuerdo con los planes de respuesta.	Parcial	1	Adaptable	4	3	Alta
		RS.CO-4: La coordinación con las partes interesadas se realiza en consonancia con los planes de respuesta.	Parcial	1	Adaptable	4	3	Alta
		RS.CO-5: El intercambio voluntario de información se produce con las partes interesadas externas para lograr una mayor conciencia situacional de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RS-CO: Comunicaciones"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Análisis (RS.AN): Se lleva a cabo el análisis para garantizar una respuesta eficaz y apoyar las actividades de recuperación.	**RS.AN-1:** Se investigan las notificaciones de los sistemas de detección.	Parcial	1	Adaptable	4	3	Alta
		RS.AN-2: Se comprende el impacto del incidente.	Parcial	1	Adaptable	4	3	Alta
		RS.AN-3: Se realizan análisis forenses.	Parcial	1	Adaptable	4	3	Alta
		RS.AN-4: Los incidentes se clasifican de acuerdo con los planes de respuesta.	Parcial	1	Adaptable	4	3	Alta
		RS.AN-5: Se establecen procesos para recibir, analizar y responder a las vulnerabilidades divulgadas a la organización desde fuentes internas y externas (por ejemplo, pruebas internas, boletines de seguridad o investigadores de seguridad).	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RS-AN: Análisis"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Mitigación (RS.MI): Se realizan actividades para evitar la expansión de un evento, mitigar sus efectos y resolver el incidente.	**RS.MI-1:** Los incidentes son contenidos.	Parcial	1	Adaptable	4	3	Alta
		RS.MI-2: Los incidentes son mitigados.	Parcial	1	Adaptable	4	3	Alta
		RS.MI-3: Las vulnerabilidades recientemente identificadas son mitigadas o se documentan como riesgos aceptados.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RS-MI: Mitigación"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Mejoras (RS.IM): Las actividades de respuesta de la organización se mejoran al incorporar las lecciones aprendidas de las actividades de detección y respuesta	**RS.IM-1:** Los planes de respuesta incorporan las lecciones aprendidas.	Parcial	1	Adaptable	4	3	Alta
		RS.IM-2: Se actualizan las estrategias de respuesta.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RS-IM: Mejoras"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
RECUPERAR (RC)	**Planificación de la recuperación (RC.RP):** Los procesos y procedimientos de recuperación se ejecutan y se mantienen para asegurar la restauración de los sistemas o activos afectados por incidentes de seguridad cibernética.	**RC.RP-1:** El plan de recuperación se ejecuta durante o después de un incidente de seguridad cibernética.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RC-RP: Planificación de la recuperación"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Mejoras (RC.IM): La planificación y los procesos de recuperación se mejoran al incorporar en las actividades futuras las lecciones aprendidas.	**RC.IM-1:** Los planes de recuperación incorporan las lecciones aprendidas.	Parcial	1	Adaptable	4	3	Alta
		RC.IM-2: Se actualizan las estrategias de recuperación.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RC-IM: Mejoras"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**
	Comunicaciones (RC.CO): Las actividades de restauración se coordinan con partes internas y externas (por ejemplo, centros de coordinación, proveedores de servicios de Internet, propietarios de sistemas de ataque, víctimas, otros CSIRT y vendedores).	**RC.CO-1:** Se gestionan las relaciones públicas.	Parcial	1	Adaptable	4	3	Alta
		RC.CO-2: La reputación se repara después de un incidente.	Parcial	1	Adaptable	4	3	Alta
		RC.CO-3: Las actividades de recuperación se comunican a las partes interesadas internas y externas, así como también a los equipos ejecutivos y de administración.	Parcial	1	Adaptable	4	3	Alta
	Resumen de la categoría "RC-CO: Comunicaciones"		**%Logro**	25,00%	**%Objetivo**	100,00%	75,00%	**%Prioridad**

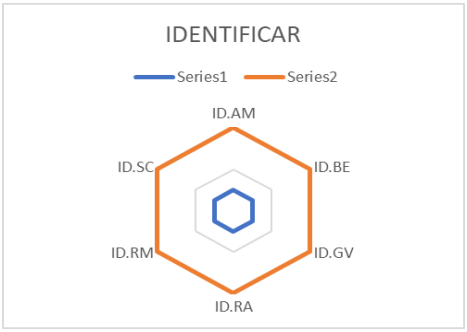
Nota. Lista de chequeo para recopilar datos y asegurar la calidad en diversos procesos, ayuda a los auditores a seguir un enfoque sistemático y a asegurarse de que no se omita ningún aspecto importante durante la revisión.

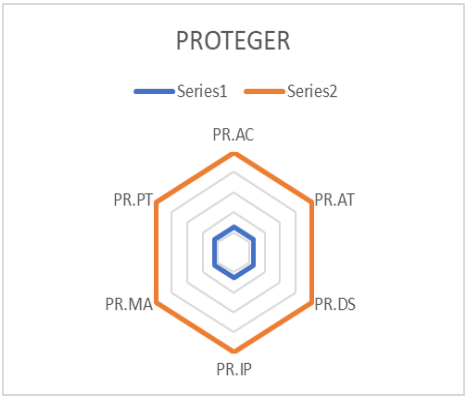
Resultados

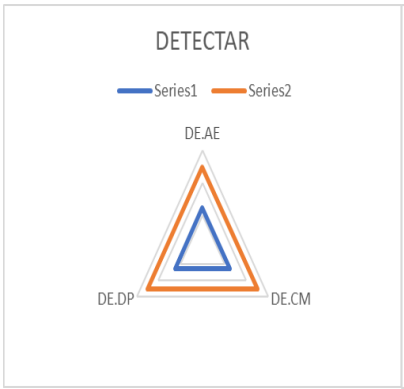
Tabla 48.

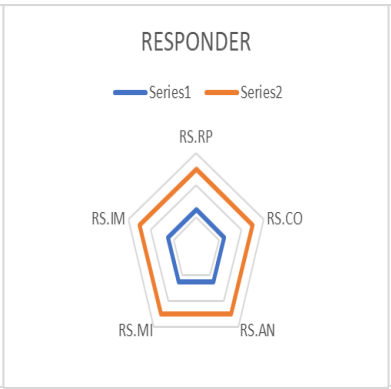
Análisis de valores

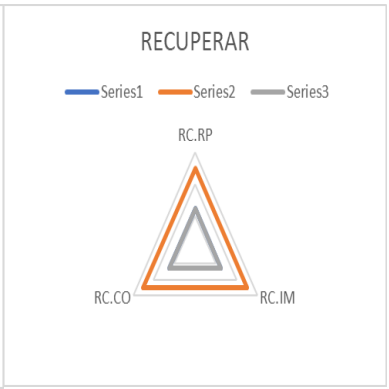
Función	Categoría	%Logro	%Objetivo	%Brecha
IDENTIFICAR (ID)	ID.AM	25,00%	100,00%	75,00%
	ID.BE	25,00%	100,00%	75,00%
	ID.GV	25,00%	100,00%	75,00%
	ID.RA	25,00%	100,00%	75,00%
	ID.RM	25,00%	100,00%	75,00%
	ID.SC	25,00%	100,00%	75,00%
Función ID		**25,00%**	**100,00%**	**75,00%**
PROTEGER (PR)	PR.AC	25,00%	100,00%	75,00%
	PR.AT	25,00%	100,00%	75,00%
	PR.DS	25,00%	100,00%	75,00%
	PR.IP	25,00%	100,00%	75,00%
	PR.MA	25,00%	100,00%	75,00%
	PR.PT	25,00%	100,00%	75,00%
Función PR		**25,00%**	**100,00%**	**75,00%**
DETECTAR (DE)	DE.AE	25,00%	50,00%	25,00%
	DE.CM	25,00%	50,00%	25,00%
	DE.DP	25,00%	50,00%	25,00%
Función DE		**25,00%**	**50,00%**	**25,00%**
RESPONDER (RS)	RS.RP	25,00%	50,00%	25,00%
	RS.CO	25,00%	50,00%	25,00%
	RS.AN	25,00%	50,00%	25,00%
	RS.MI	25,00%	50,00%	25,00%
	RS.IM	25,00%	50,00%	25,00%
Función RS		**25,00%**	**50,00%**	**25,00%**
RECUPERAR (RC)	RC.RP	25,00%	50,00%	25,00%
	RC.IM	25,00%	50,00%	25,00%
	RC.CO	25,00%	50,00%	25,00%
Función RC		**25,00%**	**50,00%**	**25,00%**











Nota. Esta tabla es útil para evaluar y monitorear el progreso en la implementación de medidas de ciberseguridad.

Tabla 49.

Hallazgos

CONTROL	DESCRIPCION
(PR.AC-1)	Ausencia de controles efectivos en la emisión, gestión y auditoría de identidades y credenciales.
(PR.AC-2)	Falta de gestión y protección adecuada del acceso físico a los activos.
(PR.AC-3)	Deficiencias en la gestión del acceso remoto.
(PR.AC-4)	Inadecuada gestión de permisos y autorizaciones de acceso.
(PR.AC-5)	Falta de protección de la integridad de la red, careciendo de prácticas como la segregación y segmentación de la red.
(PR.AC-7)	Problemas en la autenticación de usuarios, dispositivos y activos.
(PR.AT-1)	Insuficiencia en la capacitación e información de los usuarios.
(PR.DS-6)	Ausencia de mecanismos de comprobación de la integridad para software, firmware e información.
(PR.IP-3)	Falta de procesos establecidos para el control de cambio de configuración.
(PR.IP-4)	Carencia de políticas y prácticas efectivas de copias de seguridad.
(PR.IP-9)	Ausencia de planes de respuesta a incidentes y continuidad del negocio.
(PR.PT-1)	Deficiencias en la determinación y revisión de registros de auditoría.
(PR.PT-2)	Necesidad de restricciones más estrictas sobre el uso de medios extraíbles.
(PR.PT-4)	Falta de protección adecuada para las redes de comunicaciones y control.
(DE.CM-1 y DE.CM-2)	Insuficiencias en el monitoreo de eventos de seguridad cibernética.
(DE.CM-3, DE.CM-4,	Problemas en la detección y monitoreo de actividades maliciosas, conexiones no autorizadas y escaneos de vulnerabilidades.

Nota. Estos hallazgos indican áreas donde se necesitan mejoras en la seguridad y gestión de la información.

Tabla 50.

Recomendaciones y seguimiento

seguimiento a estas recomendaciones		
1. Desarrollo de Políticas y Procedimientos:	**2. Control de Acceso Físico y Remoto:**	**3. Capacitación y Concientización:**
Seguimiento del Desarrollo:	Implementación de Controles:	Programas de Formación:
• Establece un cronograma para el desarrollo de políticas y procedimientos. • Realiza revisiones periódicas para garantizar que se estén desarrollando de acuerdo con las mejores prácticas de seguridad.	• Monitorea la implementación de controles de acceso físico y remoto. • Verifica que se estén siguiendo los principios de menor privilegio y separación de funciones.	• Evalúa la efectividad de los programas de formación. • Realiza encuestas o pruebas para medir el conocimiento adquirido por los empleados.
Aprobación y Comunicación:	Revisiones de Acceso:	
• Una vez desarrolladas, asegúrate de que las políticas y procedimientos sean aprobados y comunicados a todos los involucrados.	• Realiza revisiones periódicas para asegurar que los usuarios tengan los privilegios mínimos necesarios.	
4. Integridad y Control de Cambios:	**5. Gestión de la Información:**	**6. Registro y Monitoreo:**
Implementación de Mecanismos:	Copia de Seguridad:	Auditorías Internas:
• Asegúrate de que se estén implementando mecanismos de comprobación de integridad para software, firmware e información.	• Verifica la implementación de políticas y prácticas efectivas de copias de seguridad. • Realiza pruebas de restauración para asegurar la integridad de las copias de seguridad.	• Realiza auditorías internas para revisar los registros de auditoría y garantizar el cumplimiento de la política.
		Restricciones de Medios Extraíbles:
		• Monitorea el cumplimiento de las restricciones sobre el uso de medios extraíbles.
Revisiones de Cambio:	Planes de Respuesta a Incidentes:	
		Mejora Continua:
• Realiza revisiones de cambios para garantizar que se sigan los procesos establecidos.	• Supervisa el desarrollo e implementación de planes de respuesta a incidentes y continuidad del negocio.	• Implementa cambios según sea necesario para mejorar la eficacia de los controles.
7. Revisión de la Protección de Redes:	**8. Monitoreo de Eventos y Actividades:**	**9. Evaluación Continua:**
Auditorías y Revisiones:	Implementación de Herramientas:	Revisión Periódica:
• Realiza auditorías y revisiones de seguridad en las redes para garantizar la protección de las comunicaciones y el control.	• Implementa herramientas de monitoreo para eventos de seguridad cibernética, actividades del personal, conexiones no autorizadas y escaneos de vulnerabilidades.	• Programa revisiones periódicas de todas las recomendaciones. • Ajusta las medidas según sea necesario en función de la evolución de las amenazas y la tecnología.
	Alertas y Respuesta:	
	• Configura alertas y respuestas automáticas según sea necesario.	

1. Desarrollo de Políticas y Procedimientos:

Seguimiento del Desarrollo:

- Establece un cronograma para el desarrollo de políticas y procedimientos.
- Realiza revisiones periódicas para garantizar que se estén desarrollando de acuerdo con las mejores prácticas de seguridad.

Aprobación y Comunicación:

- Una vez desarrolladas, asegúrate de que las políticas y procedimientos sean aprobados y comunicados a todos los involucrados.

2. Control de Acceso Físico y Remoto:

Implementación de Controles:

- Monitorea la implementación de controles de acceso físico y remoto.
- Verifica que se estén siguiendo los principios de menor privilegio y separación de funciones.

Revisiones de Acceso:

- Realiza revisiones periódicas para asegurar que los usuarios tengan los privilegios mínimos necesarios.

3. Capacitación y Concientización:

Programas de Formación:

- Evalúa la efectividad de los programas de formación.
- Realiza encuestas o pruebas para medir el conocimiento adquirido por los empleados.

4. Integridad y Control de Cambios:

Implementación de Mecanismos:

- Asegúrate de que se estén implementando mecanismos de comprobación de integridad para software, firmware e información.

Revisiones de Cambio:

- Realiza revisiones de cambios para garantizar que se sigan los procesos establecidos.

5. Gestión de la Información:

Copia de Seguridad:

- Verifica la implementación de políticas y prácticas efectivas de copias de seguridad.
- Realiza pruebas de restauración para asegurar la integridad de las copias de seguridad.

Planes de Respuesta a Incidentes:

- Supervisa el desarrollo e implementación de planes de respuesta a incidentes y continuidad del negocio.

6. Registro y Monitoreo:

Auditorías Internas:

- Realiza auditorías internas para revisar los registros de auditoría y garantizar el cumplimiento de la política.

Restricciones de Medios Extraíbles:

- Monitorea el cumplimiento de las restricciones sobre el uso de medios extraíbles.

Mejora Continua:

- Implementa cambios según sea necesario para mejorar la eficacia de los controles.

7. Revisión de la Protección de Redes:

Auditorías y Revisiones:

- Realiza auditorías y revisiones de seguridad en las redes para garantizar la protección de las comunicaciones y el control.

8. Monitoreo de Eventos y Actividades:

Implementación de Herramientas:

- Implementa herramientas de monitoreo para eventos de seguridad cibernética, actividades del personal, conexiones no autorizadas y escaneos de vulnerabilidades.

Alertas y Respuesta:

- Configura alertas y respuestas automáticas según sea necesario.

9. Evaluación Continua:

Revisión Periódica:

- Programa revisiones periódicas de todas las recomendaciones.
- Ajusta las medidas según sea necesario en función de la evolución de las amenazas y la tecnología.

10. Documentación y Reportes:

Mantenimiento de Documentación:

• Asegurar de que se mantenga documentación detallada sobre la implementación y seguimiento de cada recomendación.

Reportes de Seguimiento:

• Prepara informes de seguimiento para la alta dirección, destacando el progreso y cualquier área que necesite atención adicional.

Nota. Esta tabla es útil para monitorear y asegurar que las recomendaciones de auditoría se implementen de manera efectiva y oportuna.

Anexo 3: Informe Auditoria

1. OBJETIVO GENERAL:

Este informe presenta el resultado de la investigación realizada a la validación de controles para los dispositivos mínimos de un sistema industrial SCADA a través de la cual el grupo de investigación de Auditoria y Ciberseguridad verificó la existencia, cumplimiento y efectividad de las políticas de ciberseguridad y seguridad de la información, procedimientos de administración, seguridad, mantenimiento, soporte y controles existentes de tecnología, con el objetivo de identificar cuáles fueron los controles faltantes del perfil actual de ciberseguridad y cuáles son los controles que se van a proponer en el perfil objetivo que cubran las brechas de ciberseguridad, con aras de brindar un servicio oportuno y mantener un alto grado de integridad, confiabilidad, confidencialidad y disponibilidad de la información de la organización.

2. ALCANCE

El alcance de esta evaluación se basa en los controles de la norma técnica internacional CSF NIST controles que se tienen como referencia para infraestructuras críticas.

Tabla 51.

Descripción de alcance de control

Nro.	Control	Descripción del Control
1	PR.AC-1	Identidades y credenciales
2	PR.AC-2	Acceso físico a activos
3	PR.AC-4	Permisos y autorizaciones
4	PR.AC-5	Integridad de la red
5	PR.AC-7	Autenticación de usuarios
6	PR.AT-1	Usuarios informados y capacitados
7	PR.DS-6	Mecanismos de comprobación de integridad
8	PR.IP-3	Control de cambio de configuración
9	PR.IP-4	Copias de seguridad de la información
10	PR.IP-9	Planes de respuesta y recuperación
11	PR.PT-1	Registros de auditoría o archivos
12	PR.PT-2	Medios extraíbles protegidos
13	PR.PT-4	Protección de redes de comunicaciones y control
14	DE.CM-1	Monitoreo de red para eventos de seguridad
15	DE.CM-2	Monitoreo del entorno físico
16	DE.CM-3	Monitoreo de actividad del personal
17	DE.CM-4	Detección de código malicioso
18	DE.CM-7	Monitoreo de personal, conexiones y dispositivos no autorizados
19	DE.CM-8	Escaneos de vulnerabilidades

Nota. Estos son controles específicos relacionados con la seguridad y el control interno en sistemas.

Normas internacionales / Frameworks / Marcos de Referencia:

- NTC-ISO-IEC 27001:2013 “Sistemas de Gestión de la Seguridad de la Información (SGSI)” - ANEXO A (Normativo).
- GTC-ISO-IEC 27002:2013 “Guía de Implementación de la Seguridad de la Información”.

- Framework de Ciberseguridad NIST (National Institute of Standards and Technology).
- NIST Special Publication 800-53A Revisión 4 - Assessing Security and Privacy Controls in Federal Information Systems and Organizations.
- CIS CONTROLS "Center For Internet Security"
- Marco de Referencia COBIT 5 (Control Objectives for Information and related Technology).

Circulares Internas:

- Manual no oficial de Seguridad de la información y Ciberseguridad.
- Procedimiento no oficial de Políticas de Seguridad de la Información y Ciberseguridad.

Proceso verificado: Control General de Tecnología

Área: Dirección de Tecnologías de Información / Área SCADA

Periodo evaluado (dd/mm/aaaa): 01/01/2022 a 21/11/2022

3. TRABAJO REALIZADO:

- Identificar los activos, riesgos, amenazas y vulnerabilidades de los activos críticos que conforman un sistema industrial SCADA.
- Identificar la función, categoría, subcategoría y referencias informativas de los controles que faltaron al interior de la Organización. (CSF FRAMEWORK NIST)
- Se realizaron recomendaciones de controles tecnológicos para cerrar las brechas de seguridad de la información y/o ciberseguridad que se presentaron en la organización.

4. FUENTE DE INFORMACIÓN:

- La auditoría se inicia sin alguna fuente de información o actas relacionadas con anteriores procesos que fueron auditados.
- Se encuentra como fuente de información referente a procesos inconclusos de generación de políticas de seguridad y manuales de configuración mínima o estándar sobre los dispositivos.
- Se elabora un mapa de riesgos determinado en el punto 3.1.3 donde tenemos la información de los activos mínimos del sistema industrial SCADA y que tomamos de referente dado que el caso de estudio nos pide evaluar los dispositivos PLC, HMI

5. RESULTADOS OBTENIDOS:

Activos vulnerados:

- PLC.
- HMI.

Se tomaron de muestra estos 2 activos que hacen parte de los activos mínimos de un sistema industrial SCADA y que aparecen

Riesgos:
(1) -Posibilidad que la amenaza: Phishing, afecte el activo: PLC
(9) -Posibilidad que la amenaza: Malware, afecte el activo: PLC
(17) -Posibilidad que la amenaza: DoS, afecte el activo: PLC

(25) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: PLC
(33) -Posibilidad que la amenaza: Inyección de código, afecte el activo: PLC
(41) -Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: PLC
(49) -Posibilidad que la amenaza: Fallos humanos, afecte el activo: PLC
(4) -Posibilidad que la amenaza: Phishing, afecte el activo: EQUIPAMENTO PANTALLA HMI
(12) -Posibilidad que la amenaza: Malware, afecte el activo: EQUIPAMENTO PANTALLA HMI
(20) -Posibilidad que la amenaza: DoS, afecte el activo: EQUIPAMENTO PANTALLA HMI
(28) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: EQUIPAMENTO PANTALLA HMI
(36) -Posibilidad que la amenaza: Inyección de código, afecte el activo: EQUIPAMENTO PANTALLA HMI
(44) -Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: EQUIPAMENTO PANTALLA HMI
(52) -Posibilidad que la amenaza: Fallos humanos, afecte el activo: EQUIPAMENTO PANTALLA HMI

Amenazas:
A1 – Phishing.
A2 - Malware.
A3 - DoS.
A4 - Buffer overflow.
A5 - Inyección de código.
A6 - Acceso no autorizado.
A7 - Fallos humanos.

Vulnerabilidades:
V1 - Falta de concientización del personal, falta de filtros de correo electrónico, falta de segmentación en la red
V2 - Falta de actualizaciones y parches, falta de controles de acceso y autenticación, configuraciones de seguridad débiles, vulnerabilidades en software y hardware, falta de políticas y procedimientos de seguridad, fallos en la supervisión y detección de anomalías.
V3 - Falta de redundancia, configuraciones de seguridad débiles, insuficientes controles de autenticación y autorización, vulnerabilidades en el software y hardware, falta de procedimientos de respuesta a riesgos, falta de políticas de seguridad y entrenamiento del personal.
V4 - Falta de validación de entrada, Desbordamiento de búfer, Error en la gestión de memoria
V5 - Fallos de validación, falta de medidas de seguridad en la programación, falta de validación de entrada de datos.
V6 - software desactualizado, Puertos no protegidos, contraseña por defecto, falta de monitoreo
V7 - Falta de concienciación y entrenamiento del personal, errores en la configuración y operación de sistemas, falta de supervisión y detección de anomalías, falta de políticas de seguridad y procedimientos de seguridad.

De acuerdo con el mapa de riesgo presentado a continuación, sin tener en cuenta los controles (Riesgo Inherente), la mayor exposición al riesgo está concentrada en los controles: PR.AC-1 Identidades y credenciales, PR.AC-2 Acceso físico a activos, PR.AC-4 Permisos y autorizaciones, PR.AC-5 Integridad de la red, PR.AC-7 Autenticación de usuarios, PR.AT-1 Usuarios informados y capacitados, PR.DS-6 Mecanismos de comprobación de integridad, PR.IP-3 Control de cambio de configuración, PR.IP-4 Copias de seguridad de la información, PR.IP-9 Planes de respuesta y recuperación, PR.PT-1 Registros de auditoría o archivos, PR.PT-2 Medios extraíbles protegidos, PR.PT-4 Protección de redes de comunicaciones y control, DE.CM-1 Monitoreo de red para eventos de seguridad, DE.CM-2 Monitoreo del entorno físico, DE.CM-3 Monitoreo de actividad del personal,

DE.CM-4 Detección de código malicioso, DE.CM-7 Monitoreo de personal, conexiones y dispositivos no autorizados, DE.CM-8 Escaneos de vulnerabilidades. Para los activos evaluados

Para efectos de calificar el riesgo se utilizó la siguiente convención:

Riesgo Alto:
Riesgo Medio:
Riesgo Bajo:

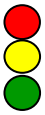


Tabla 52.

Matriz de evaluación de riesgos

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4				(9)-(12)-(17)-(20)-(25)-(28)-(33)-(41)-(44)-(49)-(53)	
Posible	3			(4) - (36)	(1) -	
Improbable	2					
Raro	1					

Nota. Esta matriz se utiliza para evaluar riesgos considerando la probabilidad de que ocurra un evento y la severidad de sus consecuencias.

Tabla 53.

Tipos de controles Tecnológicos (CFS- NIST)

Nro.	Controles Tecnológicos (CFS- NIST)	Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Nivel de Riesgo (Probabilidad x Impacto)
1	PR.PT-4 - Implementar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.	R(1) Posibilidad que la amenaza Phishing afecte el activo PLC	A1 – Phishing.	V1 - Falta de concientización del personal, falta de filtros de correo electrónico, falta de segmentación en la red.	Alta (3)	Alto (4)	**Alto** (12)
2	PR.PT-4 - Utilizar controles para proteger contra la	R(9) Posibilidad que la amenaza Malware afecte el activo PLC	A2 - Malware.	V2 - Falta de actualizaciones y parches, falta de controles de acceso y	Alta (4)	Alto (4)	**Alto** (16)

	ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.			autenticación, configuraciones de seguridad débiles, vulnerabilidades en software y hardware, falta de políticas y procedimientos de seguridad, fallos en la supervisión y detección de anomalías.			
3	PR.PT-1 - Implementar medidas para garantizar la disponibilidad y el rendimiento de los sistemas PLC incluso durante un ataque de Denegación de Servicio (DoS).	(17) -Posibilidad que la amenaza: DoS, afecte el activo: PLC	A3 - DoS.	V3 - Falta de redundancia, configuraciones de seguridad débiles, insuficientes controles de autenticación y autorización, vulnerabilidades en el software y hardware, falta de procedimientos de respuesta a riesgos, falta de políticas de seguridad y entrenamiento del personal.	Alta (4)	Alto (4)	**Alto** (16)
4	PR.PT-2 - Implementar medidas para evitar la ejecución no autorizada de código en el sistema, incluida la validación de firmas digitales para el software crítico.	(25) -Posibilidad que la amenaza: Buffer overflow, afecte el activo: PLC	A4 - Buffer overflow.	V4 - Falta de validación de entrada, Desbordamiento de búfer, Error en la gestión de memoria	Alta (4)	Alto (4)	**Alto** (16)
5	PR.PT-3 - Implementar medidas para validar y sanitizar la entrada de datos para prevenir la inyección de código malicioso.	(33) - Posibilidad que la amenaza: Inyección de código, afecte el activo: PLC	A5 - Inyección de código.	V5 - Fallos de validación, falta de medidas de seguridad en la programación, falta de validación de entrada de datos.	Alta (4)	Alto (4)	**Alto** (16)
6	PR.AC-2 - Aplicar controles de	(41) - Posibilidad que la amenaza:	A6 - Acceso no autorizad	V6 - software desactualizado, Puertos no	Alta (4)	Alto (4)	**Alto** (16)

	acceso rigurosos, incluida la autenticación de múltiples factores, para limitar el acceso a los sistemas PLC.	Acceso no autorizado, afecte el activo: PLC	o.	protegidos, contraseña por defecto, falta de monitoreo			
7	PR.AC-3 y DE.CM-8 - Implementar controles de acceso basados en roles y proporcionar capacitación y concientización regular para reducir la probabilidad de errores humanos.	(49) - Posibilidad que la amenaza: Fallos humanos, afecte el activo: PLC	A7 - Fallos humanos.	V7 - Falta de concienciación y entrenamiento del personal, errores en la configuración y operación de sistemas, falta de supervisión y detección de anomalías, falta de políticas de seguridad y procedimientos de seguridad.	Alta (4)	Alto (4)	**Alto** (16)
8	PR.PT-4 - Implementar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.	(4) -Posibilidad que la amenaza: Phishing, afecte el activo: EQUIPAMENTO PANTALLA HMI	A1 – Phishing.	V1 - Falta de concientización del personal, falta de filtros de correo electrónico, falta de segmentación en la red.	Alta (4)	Alto (4)	**Alto** (16)
9	PR.PT-4 - Utilizar controles para proteger contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.	(12) - Posibilidad que la amenaza: Malware, afecte el activo: EQUIPAMENTO PANTALLA HMI	A2 - Malware.	V2 - Falta de actualizaciones y parches, falta de controles de acceso y autenticación, configuraciones de seguridad débiles, vulnerabilidades en software y hardware, falta de políticas y procedimientos de seguridad, fallos en la supervisión y detección de anomalías.	Alta (4)	Alto (4)	**Alto** (16)
10	PR.PT-1 - Implementar	(20) - Posibilidad que	A3 - DoS.	V3 - Falta de redundancia,	Alta (3)	Alto (3)	**Alto** (9)

	medidas para garantizar la disponibilidad y el rendimiento de los sistemas PLC incluso durante un ataque de Denegación de Servicio (DoS).	la amenaza: DoS, afecte el activo: EQUIPAMENTO PANTALLA HMI		configuraciones de seguridad débiles, insuficientes controles de autenticación y autorización, vulnerabilidades en el software y hardware, falta de procedimientos de respuesta a riesgos, falta de políticas de seguridad y entrenamiento del personal.			
11	PR.PT-2 - Implementar medidas para evitar la ejecución no autorizada de código en el sistema, incluida la validación de firmas digitales para el software crítico.	(28) - Posibilidad que la amenaza: Buffer overflow, afecte el activo: EQUIPAMENTO PANTALLA HMI	A4 - Buffer overflow.	V4 - Falta de validación de entrada, Desbordamiento de búfer, Error en la gestión de memoria	Alta (4)	Alto (4)	**Alto** (16)
12	PR.PT-3 - Implementar medidas para validar y sanitizar la entrada de datos para prevenir la inyección de código malicioso.	(36) - Posibilidad que la amenaza: Inyección de código, afecte el activo: EQUIPAMENTO PANTALLA HMI	A5 - Inyección de código.	V5 - Fallos de validación, falta de medidas de seguridad en la programación, falta de validación de entrada de datos.	Alta (3)	Alto (3)	**Alto** (9)
13	PR.AC-2 - Aplicar controles de acceso rigurosos, incluida la autenticación de múltiples factores, para limitar el acceso a los sistemas PLC.	(44) - Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: EQUIPAMENTO PANTALLA HMI	A6 - Acceso no autorizado.	V6 - software desactualizado, Puertos no protegidos, contraseña por defecto, falta de monitoreo	Alta (4)	Alto (4)	**Alto** (16)
14	PR.AC-3 y DE.CM-8 - Implementar controles de acceso basados en roles y	(52) - Posibilidad que la amenaza: Fallos humanos, afecte el activo: EQUIPAMENTO PANTALLA	A7 - Fallos humanos.	V7 - Falta de concienciación y entrenamiento del personal, errores en la configuración y operación de	Alta (4)	Alto (4)	**Alto** (16)

	proporcionar capacitación y concientización regular para reducir la probabilidad de errores humanos.	HMI		sistemas, falta de supervisión y detección de anomalías, falta de políticas de seguridad y procedimientos de seguridad.			

Nota. Estos son controles específicos relacionados con la seguridad tecnológica y el control de riesgos, ayudando a prevenir ataques y aseguran que los sistemas estén protegidos contra amenazas cibernéticas.

Es importante mencionar que durante la investigación realizada no poseen ningún tipo de control con relación al CSF NIST y de ningún otra norma o buena práctica. Por esta circunstancia damos un concepto de implementar lo antes posible un SGSI (sistema de seguridad de in la información) y un SGCI (sistema de gestión de ciberseguridad industrial)

Por otra parte, se evidencian aspectos como los descritos a continuación que requieren atención en el corto plazo para disminuir los riesgos anteriormente mencionados.

El informe detallado adjunto describe la totalidad de las conclusiones y recomendaciones obtenidas.

Queremos agradecer la colaboración prestada por los colaboradores a su cargo y quedamos dispuestos a aclarar cualquier duda al respecto.

Cordialmente,

RONY CAICEDO
AUDITOR LIDER

Tabla 54.

(PR.AC-1)

Riesgo	***Hallazgo (No conformidad) / Incumplimiento) / Observación***	***Nivel de Riesgo*** *(Alto /Moderado / Bajo)*	***Recomendación / Oportunidad de mejora***	***Responsable / Cargo / Área***	***Fecha Seguimiento*** *(dd/mm/aaaa)*	***Compromiso área***
La ausencia de controles efectivos en la emisión, gestión y auditoría de identidades y credenciales en el sistema SCADA representa un riesgo significativo para la seguridad operativa y la integridad del proceso industrial. Este hallazgo señala la falta de medidas sólidas para garantizar la autenticación y autorización adecuadas, creando una brecha potencial que podría ser explotada por amenazas maliciosas	1. Vulnerabilidad a Accesos No Autorizados: • La carencia de un proceso robusto para la emisión y gestión de identidades aumenta la probabilidad de accesos no autorizados al sistema SCADA, poniendo en riesgo la confidencialidad y la integridad de los datos críticos. 2. Potencial para Manipulación de Procesos: • La falta de controles adecuados en la emisión de credenciales abre la puerta a la posibilidad de manipulación de procesos por parte de actores no autorizados, lo que podría tener consecuencias graves en la operatividad del sistema. 3. Amenazas Internas: • Sin una auditoría efectiva de identidades y credenciales, existe un riesgo latente de amenazas internas que podrían abusar de sus privilegios, comprometiendo	**Alto**	1.Implementación de Políticas de Identidad Rigurosas: • Se recomienda establecer y aplicar políticas de identidad robustas que abarquen desde la emisión hasta la revocación de credenciales, garantizando que solo individuos autorizados tengan acceso al sistema. 2. Proceso de Auditoría Regular: • Es imperativo establecer un proceso de auditoría regular de identidades y credenciales para identificar y abordar de manera proactiva cualquier anomalía o actividad sospechosa. 3. Uso de Tecnologías de Autenticación Fuertes: • La adopción de tecnologías de autenticación fuertes, como la autenticación multifactor (MFA), puede añadir una capa adicional de seguridad, mitigando el riesgo de accesos no autorizados.	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	la seguridad desde dentro del sistema.					

Nota. El control PR.AC-1 se refiere a la gestión de identidades y credenciales en un sistema.

Tabla 55.

(PR.AC-2)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La carencia de una gestión y protección adecuada del acceso físico a los activos en el sistema SCADA constituye un riesgo significativo que compromete la seguridad integral de las operaciones industriales. Este hallazgo destaca la necesidad urgente de establecer controles sólidos para salvaguardar los componentes físicos del sistema, mitigando así potenciales amenazas que podrían derivarse de accesos no autorizados.	1. Exposición a Amenazas Físicas: • La falta de una gestión adecuada del acceso físico expone los activos del sistema SCADA a posibles amenazas físicas, como daños intencionados, robo de información o manipulación no autorizada. 2. Vulnerabilidad a Accesos No Autorizados: • La ausencia de medidas de protección sólidas facilita el acceso no autorizado a áreas críticas, comprometiendo la integridad y la confidencialidad de los activos y datos sensibles. 3. Riesgo de Interrupción Operativa: • Un acceso físico no gestionado aumenta el riesgo de interrupciones operativas debido a interferencias maliciosas o	**Alto**	1. Implementación de Controles de Acceso Físico: • Se recomienda la implementación de controles de acceso físico, como sistemas de cerraduras electrónicas, tarjetas de acceso y vigilancia, para restringir el acceso solo a personal autorizado. 2. Monitoreo Continuo: • Establecer un sistema de monitoreo continuo para detectar y responder rápidamente a cualquier actividad no autorizada o intento de acceso a los activos del sistema SCADA. 3. Capacitación del Personal: • Proporcionar capacitación regular al personal sobre la importancia	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	acciones no autorizadas sobre componentes clave del sistema SCADA.		de la seguridad física y la responsabilidad compartida en la protección de los activos.			

Nota. El control PR.AC-2 se refiere al acceso físico a activos en un sistema.

Tabla 56.

(PR.AC-3)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de deficiencias en la gestión del acceso remoto en el sistema SCADA destaca un área crítica de vulnerabilidad que podría comprometer la integridad, confidencialidad y disponibilidad de los procesos industriales. Este hallazgo subraya la necesidad inmediata de establecer controles robustos para garantizar la seguridad del acceso remoto y prevenir posibles amenazas derivadas de una gestión insuficiente.	1. Aumento del Riesgo de Accesos No Autorizados: • Las deficiencias en la gestión del acceso remoto crean una apertura para posibles accesos no autorizados, poniendo en peligro la seguridad de los sistemas SCADA y la información sensible. 2. Exposición a Amenazas de Seguridad: • La falta de controles adecuados expone al sistema a amenazas como ataques de intermediarios, interceptación de datos y manipulación remota, comprometiendo la confidencialidad e integridad de la información. 3. Posible Impacto en la Disponibilidad:	**Alto**	1. Implementación de Autenticación Multifactor (MFA): • Se recomienda la adopción de autenticación multifactor para reforzar la seguridad del acceso remoto, asegurando que solo usuarios autorizados puedan acceder al sistema. 2. Establecimiento de Conexiones Seguras: • Garantizar que todas las conexiones remotas se realicen a través de canales seguros, como VPN (Red Privada Virtual), para proteger la confidencialidad de los datos durante la transmisión. 3. Monitoreo Activo del Acceso Remoto: • Implementar	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	• Una gestión ineficiente del acceso remoto aumenta el riesgo de interrupciones operativas, ya que podría facilitar ataques que afecten la disponibilidad de los sistemas críticos.		un sistema de monitoreo activo para supervisar las actividades de acceso remoto y detectar de manera proactiva cualquier actividad sospechosa o intento no autorizado.			

Nota. Este control tiene como objetivo gestionar el acceso a los sistemas desde ubicaciones remotas.

Tabla 57.

(PR.AC-4)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de una inadecuada gestión de permisos y autorizaciones de acceso en el sistema SCADA señala una brecha crítica en el control de la seguridad, comprometiendo la integridad y confidencialidad de los datos críticos del proceso industrial. Este hallazgo subraya la urgencia de implementar medidas robustas para garantizar la correcta asignación y	1. Riesgo de Accesos No Autorizados: • La gestión deficiente de permisos aumenta la probabilidad de accesos no autorizados, exponiendo el sistema a amenazas que podrían comprometer la seguridad de los datos y la integridad de los procesos. 2. Potencial para Manipulación de Datos: • La falta de autorizaciones adecuadas abre la puerta a la manipulación no autorizada de datos críticos, lo que podría tener consecuencias	**Alto**	1. Revisión y Actualización de Políticas de Autorización: • Es esencial realizar una revisión exhaustiva de las políticas de autorización, asegurando que estén alineadas con los requisitos de seguridad actuales y que reflejen la estructura organizativa del sistema SCADA. 2. Implementación de Principios de Menor Privilegio: • Adoptar el principio de menor privilegio, asignando solo	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

supervisión de permisos, mitigando así riesgos asociados con accesos no autorizados.	graves en la toma de decisiones y la operatividad del sistema. 3. Amenaza a la Confidencialidad: • La inadecuada gestión de permisos podría resultar en la revelación no autorizada de información sensible, poniendo en riesgo la confidencialidad de los datos del sistema SCADA.		los permisos necesarios para realizar tareas específicas, reduciendo así la superficie de ataque potencial. 3. Monitoreo Continuo de Permisos: • Establecer un sistema de monitoreo continuo para supervisar y auditar los permisos asignados, identificando de manera proactiva cualquier cambio no autorizado o anomalía en la gestión de autorizaciones.			

Nota. El control PR.AC-4 se refiere a la protección contra la ejecución o habilitación de código no autorizado a través de la interacción con sitios web no confiables, correos electrónicos o documentos adjuntos.

Tabla 58.

(PR.AC-5)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de una falta de protección de la integridad de la red, especialmente la ausencia de prácticas como la segregación y segmentación de la red en el sistema SCADA, representa un riesgo significativo	1. Aumento del Riesgo de Propagación de Amenazas: • La falta de segregación y segmentación de la red aumenta el riesgo de propagación rápida de amenazas dentro del sistema SCADA, comprometiendo múltiples componentes y afectando la operación	**Alto**	1. Implementación de Segregación de Red: • Se recomienda la implementación de prácticas de segregación de red para aislar áreas críticas, limitando así la propagación potencial de amenazas y reduciendo la superficie de ataque. 2. Segmentación	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

para la seguridad operativa. Este hallazgo destaca la necesidad apremiante de implementar medidas que salvaguarden la integridad de la red, reduciendo así el potencial impacto de amenazas y asegurando un entorno más resistente a ataques.	general. 2. Vulnerabilidad a Ataques Laterales: • La carencia de prácticas de segmentación permite que un atacante, una vez dentro del sistema, tenga acceso indiscriminado a diferentes áreas, lo que facilita ataques laterales y la expansión de la amenaza. 3. Dificultad en la Identificación de Anomalías: • La falta de protección de la integridad de la red dificulta la identificación temprana de anomalías y actividades sospechosas, aumentando el tiempo de respuesta ante posibles amenazas.		Lógica de la Red: • Establecer segmentación lógica de la red para dividir el sistema en zonas de confianza, garantizando que el acceso a áreas sensibles esté estrictamente controlado. 3. Monitoreo Continuo de la Integridad de la Red: • Implementar un sistema de monitoreo continuo que permita la detección proactiva de cualquier actividad anómala en la red, facilitando una respuesta rápida ante posibles amenazas.			

Nota. Este control tiene como objetivo garantizar la integridad de la red mediante prácticas como la segmentación, el monitoreo de tráfico y la protección contra intrusiones.

Tabla 59.

(PR.AC-7)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de problemas en la autenticación de usuarios, dispositivos y activos en el sistema SCADA	1. Aumento del Riesgo de Accesos No Autorizados: • Problemas en la autenticación incrementan la probabilidad de accesos no autorizados,	**Alto**	1. Implementación de Autenticación Multifactor (MFA): • Se recomienda la adopción de autenticación multifactor para	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

señala una vulnerabilidad crítica que podría comprometer la integridad y seguridad del entorno industrial. Este hallazgo destaca la necesidad inmediata de abordar las deficiencias en los mecanismos de autenticación para garantizar una sólida defensa contra accesos no autorizados.	exponiendo el sistema SCADA a amenazas que podrían comprometer la confidencialidad y disponibilidad de la información. 2. Posible Suplantación de Identidad: • Deficiencias en la autenticación podrían permitir la suplantación de identidad, facilitando a actores malintencionados el acceso no autorizado a recursos críticos del sistema. 3. Riesgo de Compromiso de Dispositivos: • Problemas en la autenticación de dispositivos pueden resultar en el compromiso de activos críticos, afectando la integridad y operación normal del sistema SCADA.		fortalecer la autenticación de usuarios, dispositivos y activos, mitigando el riesgo de accesos no autorizados. 2. Revisión y Fortalecimiento de Políticas de Contraseñas: • Realizar una revisión exhaustiva de las políticas de contraseñas, estableciendo requisitos robustos para contraseñas y garantizando su cambio periódico. 3. Monitoreo Activo de Actividades de Autenticación: • Implementar un sistema de monitoreo activo para supervisar las actividades de autenticación, identificando y respondiendo rápidamente a cualquier intento sospechoso.			

Nota. El control PR.AC-7 se refiere a la autenticación de usuarios en un sistema.

Tabla 60.

(PR.AT-1)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de una insuficiencia en la capacitación e información	1. Aumento del Riesgo de Prácticas No Seguras: • La falta de capacitación	**Alto**	1. Programas de Capacitación Regulares: • Implementar programas regulares de	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

de los usuarios en el sistema SCADA resalta un área crítica que podría comprometer la seguridad operativa. Este hallazgo subraya la importancia de mejorar la conciencia y el conocimiento de los usuarios para reducir la probabilidad de prácticas inadvertidas que puedan poner en riesgo la integridad y confidencialidad del sistema.	adecuada aumenta el riesgo de prácticas no seguras por parte de los usuarios, lo que podría resultar en errores que comprometan la seguridad del sistema SCADA. 2. Potencial para Ataques de Ingeniería Social: • La insuficiencia en la capacitación crea un entorno propicio para ataques de ingeniería social, donde los usuarios podrían ser víctimas de manipulación y divulgar información sensible. 3. Riesgo de Falta de Conciencia de Amenazas: • Usuarios insuficientemente informados podrían no estar al tanto de las amenazas actuales y las mejores prácticas de seguridad, aumentando el riesgo de caer víctimas de ataques cibernéticos.		capacitación que aborden temas de seguridad específicos del sistema SCADA, asegurando que los usuarios estén al tanto de las amenazas y medidas de seguridad. 2. Simulacros de Ataques y Entrenamiento en Ingeniería Social: • Realizar simulacros de ataques y sesiones de entrenamiento en ingeniería social para sensibilizar a los usuarios sobre posibles escenarios de amenazas y cómo reconocer y mitigar estos riesgos. 3. Campañas de Concientización Continua: • Lanzar campañas de concientización continua que refuercen la importancia de la seguridad y proporcionen información actualizada sobre las amenazas y mejores prácticas.			

Nota. El control PR.AT-1 se refiere a la capacitación e información de los usuarios en un sistema.

Tabla 61.

(PR.DS-6)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de la ausencia de mecanismos de comprobación de la integridad para software, firmware e información en el sistema SCADA destaca una vulnerabilidad significativa que podría comprometer la confiabilidad y seguridad de las operaciones industriales. Este hallazgo subraya la necesidad crítica de implementar medidas que aseguren la integridad de los componentes críticos del sistema.	1. Riesgo de Manipulación de Software y Firmware: • La ausencia de mecanismos de comprobación de integridad aumenta el riesgo de manipulación de software y firmware, lo que podría resultar en cambios no autorizados que comprometan la estabilidad del sistema SCADA. 2. Posibilidad de Infección por Malware: • La falta de verificación de la integridad facilita la posibilidad de infección por malware, que podría alterar o destruir datos y funcionalidades esenciales del sistema. 3. Compromiso de la Información Crítica: • La ausencia de controles de integridad expone la información crítica a posibles compromisos, ya que los datos podrían ser manipulados sin detección.	**Alto**	1Implementación de Firmas Digitales: • Introducir firmas digitales en el software y firmware para verificar su autenticidad e integridad, asegurando que solo las versiones autorizadas sean ejecutadas. 2. Monitoreo Continuo de Integridad: • Establecer un sistema de monitoreo continuo para detectar cambios no autorizados en el software, firmware e información crítica, permitiendo una respuesta rápida ante posibles compromisos. 3. Actualizaciones Seguras: • Garantizar que las actualizaciones de software y firmware se realicen a través de canales seguros y que estén firmadas digitalmente para prevenir la instalación de versiones maliciosas.	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

Nota. El control PR.DS-6 se refiere a la integridad de software y firmware en un sistema.

Tabla 62.

(PR.IP-3)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de la falta de procesos establecidos para el control de cambio de configuración en el sistema SCADA resalta una carencia significativa en la gestión de cambios, lo que podría poner en riesgo la estabilidad y seguridad del entorno industrial. Este hallazgo destaca la necesidad urgente de implementar procesos sólidos que controlen y gestionen de manera adecuada cualquier modificación en la configuración del sistema.	1. Riesgo de Configuraciones Erróneas: • La falta de procesos de control de cambio aumenta el riesgo de configuraciones erróneas que podrían afectar la operación normal del sistema SCADA, comprometiendo su estabilidad. 2. Posibilidad de Exposición a Vulnerabilidades: • Cambios no documentados o no autorizados podrían exponer el sistema a nuevas vulnerabilidades de seguridad, facilitando posibles ataques o explotaciones. 3. Dificultad en la Identificación de Cambios no Autorizados: • La ausencia de procesos establecidos dificulta la identificación y documentación de cambios no autorizados, prolongando el tiempo de respuesta ante posibles amenazas.	**Alto**	1. Implementación de Procesos de Control de Cambio: • Establecer procesos formales y documentados para el control de cambio de configuración, incluyendo revisiones de seguridad antes de la implementación. 2. Segregación de Funciones: • Aplicar principios de segregación de funciones para garantizar que solo personal autorizado pueda realizar y aprobar cambios en la configuración del sistema. 3. Registro Detallado de Cambios: • Mantener un registro detallado de todos los cambios realizados en la configuración, incluyendo información sobre quién realizó el cambio, cuándo y con qué justificación.	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

Nota. Este control tiene como objetivo establecer procesos para gestionar los cambios en la configuración del sistema.

Tabla 63.

(PR.IP-4)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de la carencia de políticas y prácticas efectivas de copias de seguridad en el sistema SCADA resalta una debilidad crítica en la capacidad de recuperación y protección de datos. Este hallazgo destaca la necesidad apremiante de establecer políticas sólidas y prácticas de respaldo que aseguren la integridad y disponibilidad de la información crítica del sistema.	1. Riesgo de Pérdida Irreparable de Datos: • La carencia de políticas efectivas de copias de seguridad aumenta el riesgo de pérdida irreparable de datos críticos, comprometiendo la continuidad operativa y la toma de decisiones. 2. Dificultad en la Recuperación ante Riesgos: • La falta de prácticas adecuadas de respaldo dificulta la recuperación eficiente ante riesgos como fallos del sistema, ataques de ransomware o pérdida accidental de datos. 3. Posible Exposición a Riesgos de Seguridad: • La carencia de políticas claras de copias de seguridad puede exponer el sistema a riesgos de seguridad, ya que la falta de datos respaldados podría dificultar la restauración del sistema a un	**Alto**	1. Desarrollo de Políticas de Copias de Seguridad: • Establecer políticas claras y detalladas para la realización regular de copias de seguridad, especificando la frecuencia, la retención y los procedimientos de almacenamiento seguro. 2. Automatización de Procesos de Respaldo: • Implementar sistemas de respaldo automatizado que aseguren la consistencia y puntualidad en la realización de copias de seguridad, minimizando la posibilidad de errores humanos. 3. Pruebas Regulares de Restauración: • Realizar pruebas regulares de restauración para verificar la integridad de las copias de seguridad y garantizar que los datos puedan	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	estado seguro después de un incidente.		ser recuperados de manera efectiva en caso de necesidad.			

Nota. El control PR.IP-4 se refiere a la realización, mantenimiento y prueba de copias de seguridad de la información.

Tabla 64.

(PR.IP-9)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de la ausencia de planes de respuesta a riesgos y continuidad del negocio en el sistema SCADA señala una carencia crítica en la preparación para afrontar y recuperarse de posibles riesgos de seguridad. Este hallazgo destaca la necesidad urgente de desarrollar planes formales que guíen las acciones durante eventos adversos, asegurando la rápida recuperación y la minimización del impacto operativo.	1. Mayor Tiempo de Recuperación: • La ausencia de planes de respuesta a riesgos puede resultar en un mayor tiempo de recuperación ante eventos adversos, prolongando la interrupción de las operaciones normales del sistema SCADA. 2. Riesgo de Pérdida de Datos Sensibles: • La falta de un plan de continuidad del negocio aumenta el riesgo de pérdida de datos sensibles y críticos, comprometiendo la integridad y confidencialidad de la información. 3. Dificultad en la Coordinación de Respuestas: • La carencia de un plan estructurado dificulta la coordinación	**Alto** 🔴	1. Desarrollo de Planes Formales: • Elaborar planes de respuesta a riesgos y continuidad del negocio detallados, que describan roles y responsabilidades, procedimientos de respuesta y pasos a seguir durante y después de un incidente. 2. Simulacros y Ejercicios Prácticos: • Realizar simulacros y ejercicios prácticos periódicos para poner a prueba la efectividad de los planes, identificar áreas de mejora y capacitar a los equipos para una respuesta efectiva. 3. Integración con Otros Componentes de Seguridad: • Integrar los planes de respuesta a riesgos y continuidad del negocio con otros	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	efectiva entre los equipos de respuesta a riesgos, lo que podría resultar en acciones descoordinadas o ineficientes.		componentes de seguridad, como sistemas de monitoreo y detección, para garantizar una respuesta holística y coordinada.			

Nota. El control PR.IP-9 se refiere a la respuesta a riesgos y continuidad del negocio en un sistema.

Tabla 65.

(PR.PT-1)

Riesgo	**Hallazgo (No conformidad) / Incumplimiento) / Observación**	**Nivel de Riesgo** (Alto /Moderado / Bajo)	**Recomendación / Oportunidad de mejora**	**Responsable / Cargo / Área**	**Fecha Seguimiento**	**Compromiso área**
La identificación de deficiencias en la determinación y revisión de registros de auditoría en el sistema SCADA resalta una debilidad crítica en la capacidad para supervisar y evaluar la actividad del sistema. Este hallazgo destaca la necesidad de mejorar los procesos de auditoría para garantizar una monitorización efectiva y la identificación temprana de posibles amenazas.	1. Falta de Visibilidad en Actividades del Sistema: • Las deficiencias en la determinación y revisión de registros de auditoría resultan en una falta de visibilidad sobre las actividades del sistema, lo que podría ocultar acciones maliciosas o anómalas. 2. Dificultad en la Detección de Amenazas: • La carencia de una revisión efectiva de registros dificulta la detección temprana de amenazas cibernéticas, comprometiendo la capacidad de respuesta ante posibles riesgos. 3. Riesgo de Incumplimiento Normativo: • La falta de	**Alto**	1. Mejora de Procesos de Auditoría: • Implementar mejoras en los procesos de auditoría, asegurando una determinación precisa de los eventos a registrar y estableciendo criterios claros para la revisión. 2. Automatización de Registros: • Utilizar herramientas de automatización para la generación y recopilación de registros de auditoría, facilitando la revisión y análisis eficientes de la actividad del sistema. 3. Capacitación del Personal: • Proporcionar capacitación regular al personal	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	procesos robustos de revisión de registros puede resultar en incumplimientos normativos, lo que podría tener consecuencias legales y regulatorias para la organización.		encargado de la revisión de registros, asegurando una comprensión adecuada de los eventos críticos y posibles indicadores de amenazas.			

Nota. PR.PT-1 se centra en garantizar que los registros de auditoría sean accesibles, analizables y no se vean afectados por la reducción o generación de informes.

Tabla 66.

(PR.PT-2)

Riesgo	**Hallazgo (No conformidad) / Incumplimiento) / Observación**	**Nivel de Riesgo** (Alto /Moderado / Bajo)		**Responsable / Cargo / Área**	**Fecha Seguimiento**	**Compromiso área**
La identificación de la necesidad de restricciones más estrictas sobre el uso de medios extraíbles en el sistema SCADA destaca la importancia de controlar y mitigar los riesgos asociados con el uso de dispositivos extraíbles que podrían introducir amenazas de seguridad. Este hallazgo subraya la urgencia de implementar medidas más rigurosas para proteger la integridad	1. Riesgo de Introducción de Malware: • La falta de restricciones estrictas aumenta el riesgo de introducción de malware en el sistema a través de medios extraíbles, comprometiendo la integridad y disponibilidad de los recursos. 2. Potencial para Pérdida de Datos: • El uso no controlado de medios extraíbles puede resultar en la pérdida no autorizada o accidental de datos críticos del sistema SCADA, afectando la operación normal. 3. Amenaza a la Seguridad del Sistema:	**Alto**	1. Políticas y Procedimientos Claros: • Establecer políticas y procedimientos claros que regulen el uso de medios extraíbles, especificando cuándo y cómo se pueden utilizar y aplicando restricciones según la necesidad. 2. Monitoreo Activo de Dispositivos: • Implementar un sistema de monitoreo activo que detecte y registre el uso de medios extraíbles, permitiendo una respuesta rápida ante	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

y seguridad del sistema.	• La falta de restricciones adecuadas crea una amenaza potencial a la seguridad del sistema, ya que los dispositivos extraíbles podrían utilizarse como vectores de ataque para comprometer la red.		actividades no autorizadas. 3. Control de Acceso Físico: • Reforzar el control de acceso físico a los puertos USB y otros puntos de conexión, limitando la posibilidad de conexión de dispositivos extraíbles no autorizados.			

Nota. PR.PT-2 se refiere a la protección de medios extraíbles y la restricción de su uso según la política establecida.

Tabla 67.

(PR.PT-4)

Riesgo	Hallazgo (No conformidad) / Incumplimiento) / Observación	Nivel de Riesgo (Alto /Moderado / Bajo)	Recomendación / Oportunidad de mejora	Responsable / Cargo / Área	Fecha Seguimiento	Compromiso área
La identificación de la falta de protección adecuada para las redes de comunicaciones y control en el sistema SCADA resalta una vulnerabilidad significativa que podría comprometer la integridad y disponibilidad de las operaciones industriales. Este hallazgo subraya la necesidad crítica de fortalecer las medidas de seguridad para salvaguardar las redes esenciales del sistema.	1. Riesgo de Interceptación de Datos Sensibles: • La falta de protección adecuada aumenta el riesgo de interceptación de datos sensibles en las redes de comunicaciones, comprometiendo la confidencialidad de la información transmitida. 2. Potencial para Ataques de Manipulación: • La vulnerabilidad en las redes de control podría facilitar ataques de manipulación, donde los actores malintencionados podrían alterar comandos y	**Alto**	1. Implementación de Protocolos de Seguridad: • Utilizar protocolos de seguridad robustos para la comunicación en las redes, como la implementación de capas de cifrado y autenticación fuerte. 2. Segmentación de Redes: • Aplicar estrategias de segmentación de redes para limitar la exposición y el movimiento lateral de amenazas, asegurando que un compromiso no afecte a toda	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

	controlar dispositivos críticos. 3. Amenaza a la Continuidad Operativa: • La falta de protección adecuada pone en peligro la disponibilidad del sistema SCADA, ya que las redes podrían ser objeto de ataques que interrumpan las operaciones normales.		la infraestructura. 3. Monitoreo Continuo de Redes: • Implementar soluciones de monitoreo continuo para identificar y responder rápidamente a actividades anómalas en las redes de comunicaciones y control.			

Nota. PR.PT-4 se refiere a la protección de las redes de comunicación y control.

Tabla 68.

(DE.CM-1 y DE.CM-2)

Riesgo	**Hallazgo (No conformidad) / Incumplimiento) / Observación**	**Nivel de Riesgo** (Alto /Moderado / Bajo)	**Recomendación / Oportunidad de mejora**	**Responsable / Cargo / Área**	**Fecha Seguimiento**	**Compromiso área**
La identificación de insuficiencias en el monitoreo de eventos de seguridad cibernética en el sistema SCADA resalta una carencia crítica en la capacidad para detectar y responder a posibles amenazas. Este hallazgo destaca la necesidad urgente de mejorar las capacidades de monitoreo para	1. Falta de Visibilidad en Actividades Anómalas: • Las insuficiencias en el monitoreo impiden la detección temprana de actividades anómalas, aumentando el riesgo de no identificar amenazas cibernéticas en una etapa inicial. 2. Dificultad en la Respuesta Rápida: • La carencia de capacidades de monitoreo efectivas dificulta la respuesta rápida	**Alto**	1. Implementación de Herramientas de Monitoreo Avanzadas: • Adoptar herramientas avanzadas de monitoreo de seguridad cibernética que permitan la detección proactiva de amenazas, incluyendo la monitorización de registros de eventos y el análisis de comportamientos anómalos. 2. Establecimiento de Umbrales y Alertas: • Configurar	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

garantizar una respuesta proactiva y eficiente ante eventos de seguridad.	ante eventos de seguridad, prolongando el tiempo de detección y mitigación. 3. Riesgo de Persistencia de Amenazas: • La falta de visibilidad podría permitir que amenazas persistan en el sistema sin ser detectadas, lo que aumenta el riesgo de compromisos a largo plazo.		umbrales y alertas en las herramientas de monitoreo para identificar patrones de actividad inusual y recibir notificaciones inmediatas ante posibles riesgos de seguridad. 3. Capacitación del Personal: • Proporcionar capacitación continua al personal encargado del monitoreo, asegurando que estén familiarizados con las mejores prácticas y técnicas actuales de detección de amenazas.			

Nota. DE.CM-1 se refiere a la monitorización de la red para detectar posibles eventos de ciberseguridad.

Tabla 69.

(DE.CM-3, DE.CM-4, DE.CM-7 y DE.CM-8)

Riesgo	**Hallazgo (No conformidad) / Incumplimiento) / Observación**	**Nivel de Riesgo** (Alto /Moderado / Bajo)	**Recomendación / Oportunidad de mejora**	**Responsable / Cargo / Área**	**Fecha Seguimiento**	**Compromiso área**
La identificación de problemas en la detección y monitoreo de actividades maliciosas, conexiones no autorizadas y escaneos de vulnerabilidades en el sistema SCADA resalta deficiencias críticas en la capacidad para identificar amenazas potenciales y actividades	1. Riesgo de Ataques no Detectados: • Problemas en la detección aumentan el riesgo de ataques cibernéticos no detectados, permitiendo a actores malintencionados realizar actividades maliciosas sin ser identificados. 2. Exposición a Conexiones No Autorizadas: • La falta de	**Alto**	1. Implementación de Sistemas de Detección Avanzada: • Adoptar sistemas de detección avanzada de amenazas que utilicen inteligencia artificial y análisis de comportamiento para identificar actividades maliciosas. 2. Monitoreo Continuo de	Grupo de infraestructura del sistema SCADA	1 mes después del reporte final	SCADA

anómalas. Este hallazgo subraya la urgencia de mejorar las capacidades de detección y respuesta para salvaguardar la integridad y seguridad del sistema.	monitoreo adecuado podría exponer el sistema a conexiones no autorizadas, facilitando la entrada a amenazas externas que podrían comprometer la seguridad. 3. Vulnerabilidad a Escaneos de Red: • La incapacidad para detectar escaneos de vulnerabilidades aumenta la vulnerabilidad del sistema a posibles exploraciones de seguridad que podrían ser utilizadas para identificar debilidades.		Conexiones: • Establecer un monitoreo continuo de conexiones, identificando y respondiendo rápidamente a conexiones no autorizadas o comportamientos sospechosos en la red. 3. Escaneos de Vulnerabilidades Programados: • Realizar escaneos de vulnerabilidades de manera programada y controlada para identificar posibles debilidades en la seguridad, con la debida notificación y autorización. 4. Actualización Regular de Firmas y Reglas: • Mantener actualizadas las firmas y reglas de detección para asegurar la capacidad de identificar nuevas amenazas y patrones de actividad maliciosa			

Nota. Estos elementos trabajan juntos para proteger la seguridad de la información, detectar amenazas y prevenir riesgos de ciberseguridad.

Bibliografía

[1] M. Bendel, «Índice de Inteligencia de Amenazas X-Force,» IBM España News Room., 2021.

[2] N. P. P. y. A. A. P. A. S. Nikolaev, Comparative analysis of the provisions of the standards gost r iso 19011-2012 (iso 19011: 2011) and iso 19011: 2018, vol. 28, Okhrana truda i tekhnika bezopasnosti na promyshlennykh predpriyatiyakh (Labor protection saf. procedure ind. enterprises), n.º 3, pp. 64–69, marzo de 2021, 2021, p. 39.

[3] C.-E. J. C. V.-S. D. R. &. D. A. F. O. J. C, «Redes Industriales.,» 2021.

[4] CTQAdmin. , «https://www.ctq.com.mx/objetivos-de-la-automatizacion-industrial/.,» Objetivos de la Automatización Industrial - Critical to Quality". Critical to Quality., 28 Mayo 2024. [En línea].

[5] COSO, ERM , Integrating with Strategy and Performance., Committee of Sponsoring Organizations of the Treadway Commission., 2021, pp. 83-88., 2021.

[6] D. A. Rivera y J. G. Z. Aguilera, «Sistema SCADA UNAH para eficiencia energética",» Rev. Cienc. Tecnol., pp. 97–109, 2023.

[7] D. E. Acosta, Guía rápida para entender el marco de trabajo de ciberseguridad del NIST, 2017.

[8] E. Pérez-López, «Los sistemas SCADA en la automatización industrial",» *Punto de vista de Deloitte y Fortinet respecto a la ciberseguridad en organizaciones.*

[9] D. Landoll, «The IT / Digital Legal Companion: A Comprehensive Business Guide to Software, IT, Internet,,» Media and IP Law. Syngress., 2015, pp. 1-8..

[10] Satori, «Cybersecurity Frameworks,» 2022.

[11] G. Barona López y L. E. Velasteguí, «Automatización de procesos industriales mediante Industria 4.0",» AlfaPublicaciones, vol. 3, n.º 3.1, pp. 84–101, agosto de 2021., 2019.

[12] ISACA., COBIT, «Framework: Governance and Management Objectives. Information Systems Audit and Control Association., 2019.,» Information Systems Audit and Control Association., 2019.

[13] NIST , « Marco para la mejora de la seguridad cibernética en, 2018.,» Instituto Nacional de Estándares y Tecnología NIST, , 2018.

[14] UNIR, «Auditoría de seguridad informática,» 2022.

[15] J. Durana, «Automatizacion de Procesos Industriales,» https://www.academia.edu/39351171/Automatizacion_de_Procesos_Industriales., 2019.

[16] J. F. Cayo-León y R. F. Silva-Caicedo, «Sinergia entre automatización y seguridad laboral en trabajos industriales,» https://doi.org/10.35.

[17] J. E. Arias Torres, «Riesgos a los sistemas SCADA, en empresas colombianas,,» Universidad Piloto de Colombia,, 2014.

[18] V. P. M. A. y. A. H. K. Stouffer, «Guide to Industrial Control Systems (ICS) Security, NIST.SP.800-82r2, 2015.,» NIST.SP.800-82r2, 2015., 2015.

[19] L. Mertz, «Cyberattacks on Devices Threaten Data and Patients: Cybersecurity Risks Come with the Territory. Three Experts Explain What You Need to Know”,,» IEEE Pulse, vol. 9, n.º 3, pp. 25–28, mayo de 2018., 2018.

[20] Z. Ben Rhouma y Y. Boujelbene, «Internal audit planning process, automated by workflow and compliant with ISO 9001 and ISO 19011”, Rev. Eur. Droit Soc., vol. 58, n.º 1, pp. 118–131, .,» Rev. Eur. Droit Soc., vol. 58, n.º 1, pp. 118–131, dicie, 2022.

[21] T. Q. S, Z. J. J y M. H. . Vargas, «Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman”,,» TecnoLógicas, vol. 23, n.º 48, pp. 249–267,, 2020.

[22] NQA, «Guía completa para la norma ISO 27001,» 2016.

[23] F. S. M. Mafla, «Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona,» 2024.

[24] NIST., Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, vol. 05, 2021, pp. 61-72.

[25] M. Bendel, «Índice de Inteligencia de Amenazas X-Force: el sector industrial se llevó la peor parte de los ciberataques en 2021, lo que agravó los problemas de las cadenas de suministro,» IBM España News Room. , 2020.

[26] Checkpoint, «¿Qué es el Top 10 de OWASP?,» 2021.

[27] G. B. L. y. L. E. Velasteguí, «Automatización de procesos industriales mediante Industria 4.0”,,» AlfaPublicaciones, vol. 3, n.º 3.1, pp. 84–101, https://doi.org/10.33262/ap.v3i3., 2021.

[28] ISACA., COBIT , COBIT 2019 Framework: Governance and Management Objectives. Information Systems Audit and Control Association., 2019.

[29] J. K. A. Mogollón, «Importancia del sistema de gestión de seguridad,» 2022.

[30] F. A. .. R. A. Torres Valero, «. Medina Becerra, y M. Ángel . Mendoza Moreno, «Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA», Ing.USBMed, vol. 11, n.º 2, pp. 62–70, oct. 2020,» USBMed, vol. 11, n.º 2, pp. 62–70, oct. 2020, 2020.

[31] R. A. Torres Valero, «Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA”,,» Ing. USBMed, vol. 11, n.º 2, pp. 62–70, octubre de 2020., 2012.

[32] Globalsuitesolutions, «Qué es GRC? Gobierno, riesgo y cumplimiento,» 2023.

[33] ISO, «ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection,» 2022.

[34] ISO, «NORMA ISO 19011:2018 Directrices para la Auditoría de Sistemas de Gestión,» 2019.

[35] UPSIN, «Interfaz Humano Máquina (HMI).,» Repositorio Institucional de la Universidad Politécnica del Sur de Sinaloa,, 2019.

[36] G. Krueger, «Normas para la seguridad de la información: una visión general,» dqsglobal, 2022.

[37] ISO, «ISO/IEC 27002:2013.,» 2013.

[38] Isotools, «Nueva ISO/IEC 27002:2022: cambios con respecto a la versión de 2013,» 2023.

[39] NQA, «GUÍA DE TRANSICIÓN ISO 27001:2022,» 2022.

[40] ISO, «Estandar Internacional Iso / Iec 27005,» de *vol. 2018*, 2005, pp. 1-170.

[41] Globalsuitesolution, «¿Qué es NIST Cibersecurity Framework?,» 2023.

[42] PWC, «El NIST lanza la versión 2.0 del marco de ciberseguridad,» 2022.

[43] M. Flores Miranda, «Todo sobre NIST SP 800-53:,» 2024.

[44] NIST, «NIST SP 800-53 Rev. 5,» 2023.

[45] M. Sachez, «Infraestructuras Críticas y Ciberseguridad,» 2015.

[46] S. A. Berdugo, «La infraestructura critica en colombia,» 2018.

[47] MesAutmation, «Qué es un sistema SCADA, para qué sirve y cómo funciona,» 2019.

[48] L. Pereira, «La importancia de la ciberseguridad en la protección de las infraestructuras energéticas,» 2023.

[49] A. Aguirre, «Ciberseguridad en Infraestructuras Críticas,» 20'21.

[50] P. W. y. B. W. R. Czechowski, Seguridad cibernética en la comunicación de sistemas SCADA utilizando IEC 61850, Polonia, 2015.

[51] R. B. W. A. e. all, «Metodologías de evaluación del riesgo en ciberseguridad aplicadas a sistemas SCADA para compañías eléctricas,» *Revista Espacios*, vol. 41, nº 07, p. 27, 19 07 2020.

[52] FLAI, «El modelo de las tres líneas del IIA 2020,» 2020.

[53] Z. y. V. Quiroz, «Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman,» 2020.

[54] R. A. T.-V. e. all, «Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA,» *Ingenierías USBMed,* vol. 11, nº 2, pp. 62-67, 2020.

[55] A. A. Alina Andronache, Resiliencia bajo la prospectiva estratégica: los efectos de la gestión de la ciberseguridad y la alineación de la gestión de riesgos empresariales, 2019.

[56] Instituto Nacional de Estándares y Tecnología NIST, Marco para la mejora de la seguridad cibernética en, 2018.

[57] D. E. Acosta, «Guía rápida para entender el marco de trabajo de ciberseguridad del NIST,» 11 01 2017. [En línea]. Available: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/. [Último acceso: 03 05 2022].

[58] Centro de conocimiento, La fabrica de los pensaminetos instituto de auditores de españa, Ciberseguridad una guia de supervision, 2016.

[59] G. S. Alderete, *rol de auditor interno para evaluar la gestion de riesgo de ciber segurida,* costa rica, 2017.

[60] ISACA, «Auditando sistemas industriales e infraestructuras críticas,» El Capítulo de Madrid de ISACA, madrid, 2020.

[61] H. F. V. Montoya, Propuesta para la planeación e emplementación de un SGSI basado en la ISO/IEC 27001:2005 para una empresa de telecomunicaciones, 2014.

[62] Instituto Nacional de Estándares y Tecnología (NIST), Framework for Improving Critical Infrastructure Cybersecurity, https://nvlpubs.nist.gov/nistpubs/CSF/NIST.CSF.1.1.pdf, 2018.

[63] Theiia, «EL MODELO DE LAS TRES LÍNEAS DEL IIA 2020,» 2021.

[64] C. I. J. B. J. A. F. L. O. Ynzunza, «El entorno de la industria 4.0: implicaciones y perspectivas futuras,» Conciencia tecnológica, n.o 54, pp. 33-45, 2017.