Vulnerabilidades y amenazas emergentes en los niveles de control y supervisión de la pirámide CIM en los sistemas de control industrial (ICS): Identificación, análisis y estrategias de mitigación

Carlos Andrés Erazo Pino

Asesor

Alexander Larrahondo Nuez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Agradecimientos

Deseo expresar mi más sincero agradecimiento a todas las personas que colaboraron con la realización de este trabajo, brindando su apoyo técnico, académico y humano.

En primer lugar, agradezco al Ingeniero Alexander Larrahondo Nuez, quien se desempeñó como director de este trabajo de grado, por su valiosa orientación, su compromiso y su labor como asesor, que resultaron muy importantes para la consolidación de este proyecto.

De igual forma extiendo mi gratitud al Ingeniero Christian Hernán Obando, por sus aportes como revisor crítico, cuyas observaciones y recomendaciones enriquecieron la calidad del contenido técnico y académico del documento.

A todos los ingenieros que me guiaron durante el desarrollo de cada una de las materias de la especialización en seguridad informática, les agradezco profundamente por su dedicación, experiencia y disposición para compartir sus conocimientos, los cuales fueron muy importantes para la construcción de este documento.

También reconozco el apoyo institucional de la Universidad Nacional Abierta y a Distancia – UNAD, así como los recursos bibliográficos, tecnológicos y materiales puestos a disposición para el desarrollo de este trabajo, que permitieron realizar un análisis riguroso y pertinente.

A todos ustedes, gracias por ser parte de este camino de formación y crecimiento profesional.

Dedicatoria

A Dios, por ser mi guía y fortaleza en cada paso de este camino, iluminando mi mente y corazón para alcanzar este logro.

A mi madre, Alejandrina Pino y a mi padre, Julio César Erazo, por su amor incondicional y por creer en mí incluso en los momentos más desafiantes. Su apoyo ha sido el pilar fundamental para alcanzar todas las metas que me he propuesto.

A mis hermanos, Leider Erazo y Ferley Erazo, por ser mi inspiración y ejemplo de perseverancia. Su lucha diaria me ha enseñado a nunca rendirme.

A mi familia, por brindarme un hogar lleno de amor, comprensión y un ambiente que siempre me impulsó a crecer.

A mis compañeros, quienes se convirtieron en grandes amigos y compartieron conmigo momentos de aprendizaje, esfuerzo y crecimiento.

A todos mis tutores y a cada persona que, de una u otra forma, contribuyó a que este sueño se hiciera realidad. Este logro es también un reflejo de su apoyo y confianza.

Con profunda gratitud,

Carlos A. Erazo P.

Resumen

La creciente digitalización y conectividad de los Sistemas de Control Industrial (ICS) han traído consigo beneficios significativos en términos de eficiencia y automatización. Sin embargo, esta evolución ha incrementado la exposición a ciberamenazas que pueden comprometer la continuidad operativa y la seguridad de sectores esenciales como la energía, la manufactura y el transporte. Esta monografía tiene como objetivo analizar las vulnerabilidades y amenazas emergentes que afectan la seguridad de los ICS, especialmente en componentes críticos como PLC (Controladores Lógicos Programables), SCADA (Sistema de Control y Adquisición de Datos) y DCS (Sistema de Control Distribuido) y redes del entorno industrial, A través de la identificación y el análisis de los riesgos y puntos críticos de los ICS, se proponen estrategias de mitigación basadas en segmentación de redes, gestión de parches y controles de acceso físico.

Estas medidas buscan fortalecer la resiliencia de las infraestructuras industriales ante ataques cibernéticos, minimizando el impacto potencial sobre la producción, la seguridad humana y el medio ambiente. El estudio se basa en un análisis documental y casos de estudio, proporcionando lineamientos que contribuyan a la protección integral de los ICS y a la continuidad operativa de procesos industriales críticos.

Palabras clave: SCI (Sistemas de Control Industrial), vulnerabilidades cibernéticas, seguridad de ICS, PLC (Controladores Lógicos Programables), SCADA (Sistema de Control y Adquisición de Datos).

Abstract

The increasing digitalization and connectivity of Industrial Control Systems (ICS) have brought significant benefits in terms of efficiency and automation. However, this evolution has also increased exposure to cyber threats that can compromise the operational continuity and security of essential sectors such as energy, manufacturing, and transportation. This monograph aims to analyze the emerging vulnerabilities and threats affecting ICS security, particularly in critical components such as PLCs (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition), and DCS (Distributed Control Systems), as well as in the convergence between IT (Information Technology) and OT (Operational Technology).

Through the identification and analysis of risks and critical points in ICS, mitigation strategies are proposed based on network segmentation, patch management, and physical access controls. These measures seek to strengthen the resilience of industrial infrastructures against cyberattacks, minimizing the potential impact on production, human safety, and the environment. The study is based on documentary analysis and case studies, providing guidelines that contribute to the comprehensive protection of ICS and the operational continuity of critical industrial processes.

Keywords: ICS (Industrial Control Systems), cyber vulnerabilities, ICS security, PLC (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition).

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La creciente interconexión de los sistemas de control industrial (ICS) ha mejorado la eficiencia en sectores críticos como energía y manufactura, pero también los ha expuesto a amenazas cibernéticas. Componentes como PLC, SCADA y DCS, diseñados para operación continua, carecen de medidas de seguridad robustas, lo que los hace vulnerables a ataques como ransomware y explotación de vulnerabilidades. Incidentes como el ataque de ransomware a Colonial Pipeline en 2021, que afectó el suministro de combustible en EE.UU, provocando desabastecimiento de combustible y pérdidas millonarias. Asimismo, el malware Triton, que comprometió sistemas de seguridad industrial en plantas petroquímicas, evidenció la capacidad de los ciberdelincuentes para manipular directamente mecanismos diseñados para proteger vidas humanas y entornos industriales. Según el informe de ciberseguridad de Dragos, en 2023 se identificó un aumento del 87 % en los ataques de ransomware contra organizaciones industriales, reflejando una tendencia creciente de amenazas en entornos industriales (Dragos, 2025).

Proteger los ICS es una prioridad, ya que gestionan infraestructuras críticas vitales para la sociedad. Sin embargo, su operación continua dificulta la implementación de medidas de seguridad tradicionales, como actualizaciones de software. Esto los convierte en objetivos atractivos para ciberdelincuentes, cuyos ataques pueden tener consecuencias graves, desde interrupciones de servicios hasta desastres ambientales.

Este proyecto analiza las vulnerabilidades y amenazas en los ICS, enfocándose en componentes críticos. Propone estrategias de mitigación, como segmentación de redes y gestión de parches, para fortalecer la resiliencia de estos sistemas y garantizar su operación segura, protegiendo así las infraestructuras críticas de las que depende la sociedad.

Planteamiento del problema

En los últimos años, los sistemas de control industrial (ICS) han evolucionado de entornos aislados y controlados a sistemas interconectados y dependientes de redes de comunicación, especialmente con la convergencia entre las tecnologías de la información (IT) y las tecnologías operativas (OT). Esta convergencia ha permitido mejorar la eficiencia y la integración operativa en sectores industriales críticos como energía, manufactura, transporte y distribución de agua, pero también ha expuesto a los ICS a una gama de amenazas cibernéticas emergentes. Los ICS, que incluyen componentes como PLC (Controladores Lógicos Programables), SCADA (Supervisión, Control y Adquisición de Datos) y DCS (Sistemas de Control Distribuido), fueron diseñados principalmente con el propósito de asegurar la continuidad operativa y la eficiencia, sin incorporar medidas de ciberseguridad adecuadas (Quiroz Tascón et al., 2020).

La creciente incorporación de dispositivos IoT y la conexión de los ICS a redes IT han abierto múltiples vectores de ataque, facilitando que los ciberdelincuentes exploten vulnerabilidades tanto en el hardware como en el software de estos sistemas. Según un informe de Trend Micro del año 2021, el 72% de las empresas industriales han sufrido al menos seis ciberataques en un año, con un costo financiero promedio de 2,8 millones de dólares por incidente (Trend Micro, 2022).

Estos ataques pueden variar desde ransomware y explotación de vulnerabilidades de día cero hasta técnicas de ingeniería social dirigidas a operadores, buscando acceder a información sensible o controles críticos. Las consecuencias incluyen interrupciones operativas, daños a la infraestructura, robo de información confidencial e incluso riesgos para la vida humana.

En el desarrollo de esta monografía, se explorarán cómo las vulnerabilidades emergentes impactan la seguridad de los Sistemas de Control Industrial (ICS). Estas vulnerabilidades exponen a los ICS a amenazas de actores externos y agentes malintencionados que pueden comprometer su integridad y disponibilidad. Estas situaciones conllevan riesgos significativos, como interrupciones en la producción, pérdidas económicas considerables y amenazas a la seguridad de los trabajadores.

Los ataques a los ICS pueden tener consecuencias graves debido a la naturaleza crítica de los procesos que controlan. La explotación de vulnerabilidades en estos sistemas puede generar fallas operativas, daños físicos en los equipos, e incluso provocar impactos ambientales, como en el caso de la manipulación de un sistema de tratamiento de agua, donde un ataque podría afectar la calidad y seguridad del suministro (Al Ghazo & Kumar, 2024).

Este problema de investigación busca no solo comprender el impacto de las vulnerabilidades y amenazas emergentes en los ICS, sino también proponer soluciones que mitiguen los riesgos asociados, garantizando una operación segura y continua de estos sistemas.

Justificación

La importancia de proteger los sistemas de control industrial es indudable, dada su función en la regulación de infraestructuras críticas que sustentan el funcionamiento de la sociedad moderna. Los ICS son componentes importantes en sectores como la energía, el agua, el gas y la manufactura, entre otros. Estos sistemas controlan procesos que, en caso de verse interrumpidos o comprometidos, pueden tener consecuencias en la seguridad pública, la economía y el bienestar de las comunidades.

La transformación de entornos aislados a sistemas interconectados ha sido motivada por la búsqueda de eficiencia operativa y de mayor capacidad de análisis y monitoreo (Muller et al., 2022). Sin embargo, esta convergencia IT-OT también ha abierto la puerta a una amplia gama de amenazas cibernéticas que los ICS no están preparados para enfrentar. A diferencia de las redes de IT convencionales, en las que las vulnerabilidades pueden ser abordadas con actualizaciones regulares y medidas de seguridad avanzadas, los ICS enfrentan limitaciones adicionales.

Lo anterior dado a que estos sistemas suelen operar 24/7 en entornos críticos, cualquier interrupción o cambio en su configuración puede tener un costo elevado o causar interrupciones en la producción, dificultando la implementación de medidas de ciberseguridad tradicionales.

En la realización de esta monografía se tiene contemplado tocar temas importantes en SCI tales como:

Protección de infraestructuras críticas: Los ICS gestionan infraestructuras críticas. Por lo que la explotación de sus vulnerabilidades puede resultar en la interrupción de servicios esenciales o en el peor de los casos, en desastres de grandes proporciones. La protección de estas infraestructuras es importante para la seguridad nacional y la estabilidad económica (Zanasi et al., 2022).

Conciencia sobre las amenazas emergentes: A medida que las tecnologías evolucionan, también lo hacen las tácticas y herramientas empleadas por los atacantes. En este sentido, esta investigación busca concienciar sobre las amenazas emergentes, incluyendo ciberataques avanzados y técnicas de ingeniería social y su capacidad de comprometer los sistemas de control industrial.

Falta de protocolos de seguridad adecuados en ICS: Muchos ICS siguen operando con poca o ninguna protección contra ataques cibernéticos. Esta monografía ayuda a identificar las principales vulnerabilidades y proponer estrategias de mitigación específicas para este entorno, promoviendo un enfoque de ciberseguridad que equilibre la necesidad de protección con la continuidad operativa de los sistemas.

Esta monografía pretende contribuir al conocimiento sobre las vulnerabilidades y amenazas en los ICS, además de proponer algunas estrategias de mitigación para ayudar a fortalecer la resiliencia de los ICS.

Objetivos

Objetivo General

Analizar las vulnerabilidades y amenazas emergentes en los niveles de control y supervisión de la pirámide CIM en los sistemas de control industrial (ICS) mediante el estudio de casos documentados y la identificación de riesgos críticos, con el fin de proponer estrategias de mitigación que garanticen su operación segura y continua.

Objetivos Específicos

Identificar las vulnerabilidades más comunes en los sistemas de control industrial (ICS), enfocándose en los riesgos asociados a componentes como PLC, SCADA y DCS, así como en las redes usadas en el entorno industrial, para determinar los principales puntos de debilidad.

Evaluar el impacto de la explotación de vulnerabilidades en ICS, considerando interrupciones operativas, daños físicos y posibles filtraciones de información crítica, con base en casos de estudio que permitan medir las consecuencias en la seguridad de infraestructuras industriales.

Proponer estrategias de mitigación basadas en la segmentación de redes, gestión de parches y controles de acceso físico, para garantizar la continuidad y seguridad operativa de los sistemas de control industrial.

Marco Referencial

Antecedentes

Los sistemas de control industrial (ICS) han evolucionado desde su inicio, pasando de ser entornos cerrados y aislados a infraestructuras interconectadas que dependen en gran medida de las redes de comunicación. Esta transformación ha permitido optimizar procesos industriales, mejorar la eficiencia operativa y facilitar la supervisión remota; sin embargo, también ha traído nuevos desafíos en términos de ciberseguridad, exponiendo estos sistemas a una gama cada vez mayor de amenazas digitales.

Inicialmente, los ICS fueron diseñados para operar en entornos completamente segregados, donde la seguridad se basaba en el aislamiento físico en lugar de en mecanismos robustos de protección digital (Quiroz Tascón et al., 2020). También destaca que estos sistemas no fueron concebidos con una arquitectura de ciberseguridad avanzada, ya que en su origen no se anticipaba la necesidad de defensa contra amenazas externas. Sin embargo, la digitalización y la integración con redes corporativas han eliminado esta barrera natural, incrementando exponencialmente el riesgo de ataques dirigidos.

La convergencia entre las tecnologías de la información (IT) y las tecnologías operativas (OT) ha sido otro componente clave en la expansión de la superficie de ataque. Al Ghazo & Kumar (2024) explican que la interconexión de estos dos mundos ha generado nuevas vulnerabilidades, ya que los ICS ahora dependen de protocolos de comunicación y sistemas que tradicionalmente pertenecían al ámbito de IT. Esta fusión ha permitido que los ciberdelincuentes exploten vulnerabilidades tanto en hardware como en software, comprometiendo la estabilidad y seguridad de infraestructuras críticas.

Además, la introducción de dispositivos del Internet de las Cosas (IoT) en entornos industriales ha multiplicado los puntos de acceso para potenciales ataques. Muller et al. (2022) advierten que el creciente uso de IoT dentro de los ICS ha abierto múltiples vectores de amenaza, facilitando ataques más sofisticados. Estos dispositivos, en muchos casos, carecen de medidas de seguridad adecuadas y pueden ser utilizados como puertas de entrada para comprometer redes enteras de control industrial.

En este contexto, la ciberseguridad de los ICS se ha convertido en una prioridad, dado que estos sistemas sustentan infraestructuras críticas como redes eléctricas, plantas de tratamiento de agua, refinerías y procesos de manufactura. La historia reciente ha demostrado que ataques dirigidos contra ICS pueden tener consecuencias devastadoras, desde interrupciones en la producción hasta daños físicos en equipos y riesgos para la seguridad de las personas. Ante este panorama, resulta pertinente desarrollar estrategias de seguridad robustas que protejan estos sistemas de las crecientes amenazas cibernéticas.

Marco conceptual

En la era digital la industrialización ha experimentado una transformación radical, gracias a la integración de tecnologías de la información (IT) en los procesos de producción. Los Sistemas de Control Industrial (ICS), que antes operaban de forma aislada, ahora se encuentran interconectados, lo que ha mejorado la eficiencia y la productividad. Sin embargo, esta convergencia entre el mundo físico y el digital ha expuesto a los ICS a una amplia gama de ciberamenazas que ponen en riesgo la continuidad de las operaciones, la seguridad de los activos y la integridad de los datos (Hotellier et al., 2024).

Este marco conceptual tiene como objetivo analizar los ICS, sus componentes clave (PLC, SCADA, DCS) y las vulnerabilidades inherentes a estos sistemas. Revisaremos cómo la

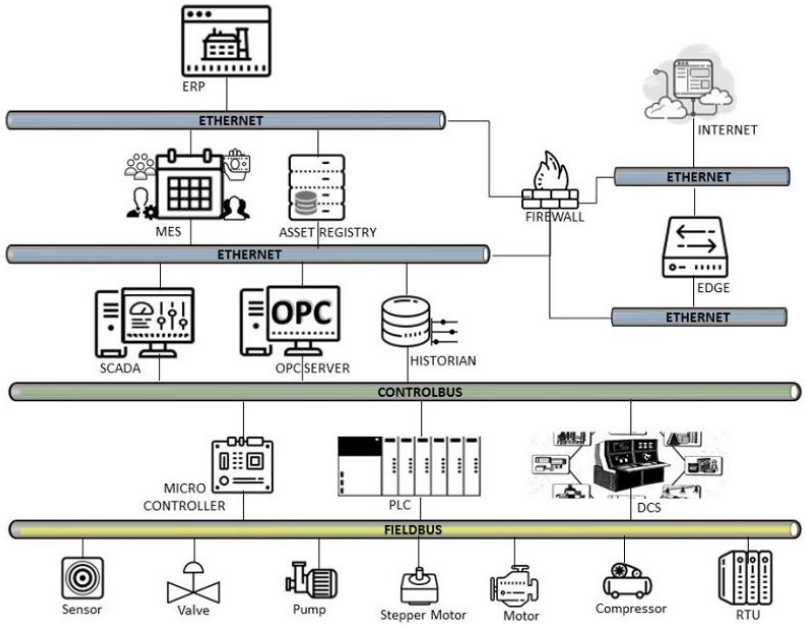
convergencia IT-OT ha ampliado la superficie de ataque y ha dado lugar a nuevas amenazas, como los ciberataques avanzados, la ingeniería social y la explotación de dispositivos IoT industriales.

Los sistemas de Control Industrial (ICS)

Los sistemas de control industrial son un conjunto de tecnologías que permiten la supervisión, el control y la automatización de procesos industriales. Se utilizan ampliamente en sectores como energía, manufactura, transporte y servicios públicos (agua y gas) para monitorear y gestionar infraestructuras críticas. Su función principal es garantizar la operación eficiente y segura de estos procesos en tiempo real, mediante la recolección y análisis de datos y la ejecución de comandos de control sobre los dispositivos de campo.

Figura 1

Esquema de un SCI típico



Nota. Estructura de la planta de automatización industrial. Tomado de https://ignaciogavilan.com/estructura-de-la-planta-de-automatizacion-industrial/

Funcionamiento de los ICS

Los ICS operan en ciclos de control de procesos que involucran la recolección de datos, el procesamiento de esos datos en tiempo real y la ejecución de comandos para ajustar los parámetros del proceso. Por ejemplo, en una planta de energía, los sensores monitorean variables como temperatura, presión y flujo, esta información se envía a los PLC o DCS que toman decisiones automáticas en función de los valores predeterminados (Adeyanju et al., 2021).

El sistema SCADA centraliza esta información, permite a los operadores monitorear el estado general del proceso y hacer ajustes manuales en caso necesario.

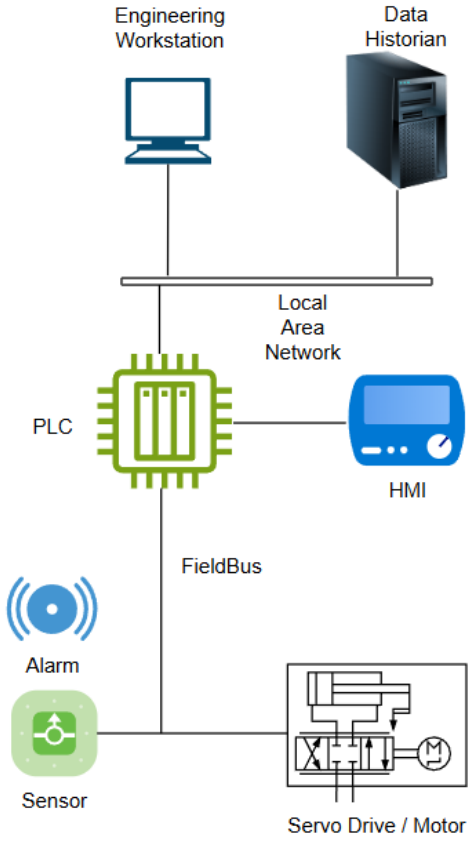
Componentes Principales de los ICS

Los ICS abarcan varias tecnologías y arquitecturas específicas, diseñadas para manejar distintos tipos de operaciones industriales. Los componentes más comunes incluyen:

PLC (Programmable Logic Controller). Los controladores lógico programables son dispositivos electrónicos programables que ejecutan secuencias de control y automatización en maquinaria y equipos industriales. Están diseñados para operar en ambientes hostiles y realizar funciones repetitivas de control de procesos (por ejemplo, encender y apagar una válvula o motor en función de un sensor). Los PLC son el primer nivel de control en muchos ICS y son críticos para la automatización de tareas específicas. Su vulnerabilidad principal radica en que, al ser diseñados inicialmente para entornos aislados, algunos carecen de medidas avanzadas de ciberseguridad.

Figura 2

Topología basada en PLC



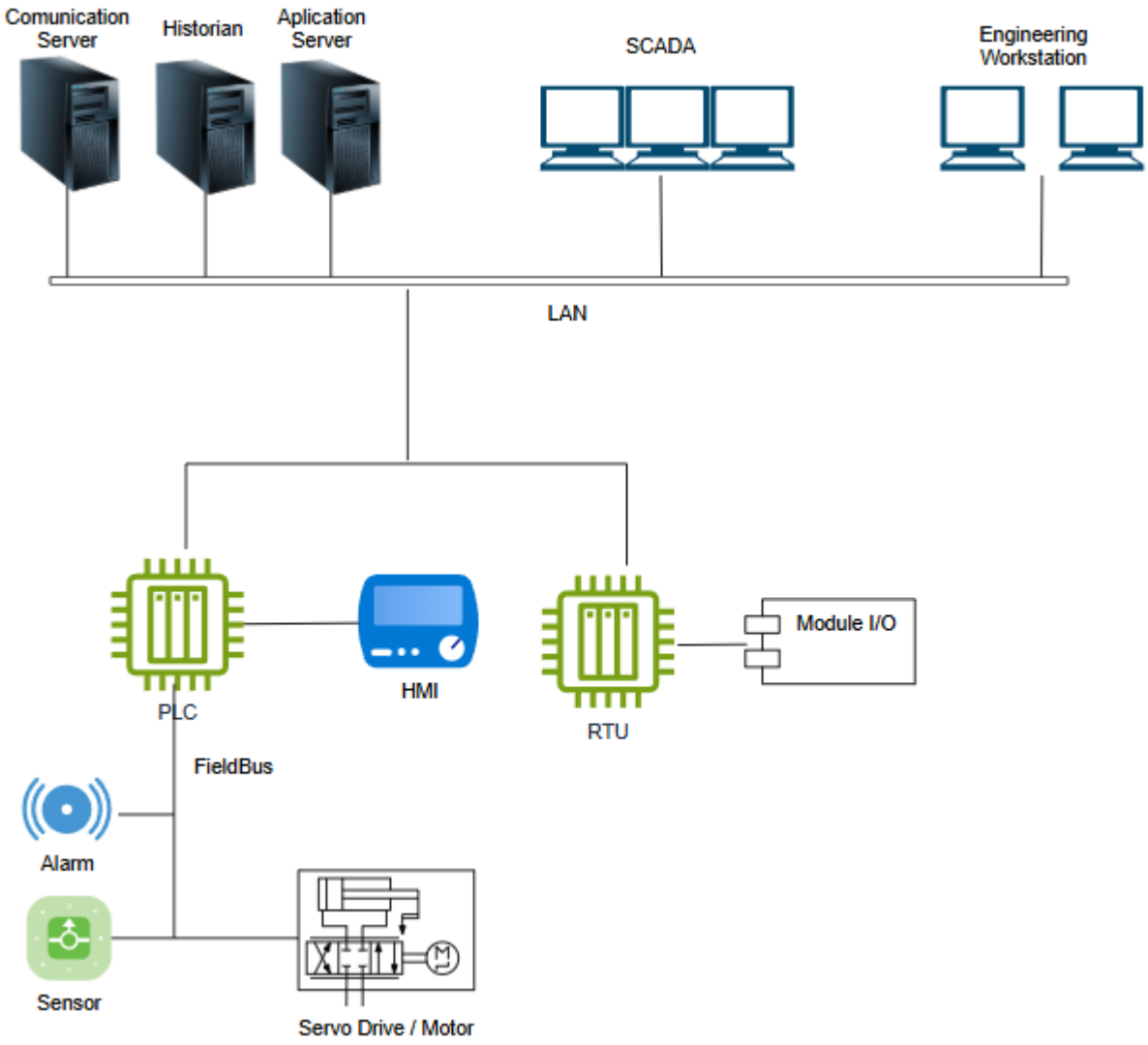
Nota. En la figura se muestra una topología basada en PLC.

SCADA (Supervisory Control and Data Acquisition). Un SCADA es una arquitectura de supervisión que se utiliza en sistemas distribuidos, como redes de distribución de agua, electricidad, gas o empresas de fabricación. Un sistema SCADA permite a los operadores monitorizar y controlar procesos industriales a distancia mediante la recopilación de datos en tiempo real. Los datos se envían a un centro de control donde se procesan y visualizan en paneles de monitoreo. Debido a su naturaleza distribuida y a su dependencia de redes de comunicación,

los sistemas SCADA son vulnerables a ciberataques que busquen interrumpir las comunicaciones o manipular los datos operativos (Quiroz Tascón et al., 2020).

Figura 3

Diseño General del Sistema SCADA



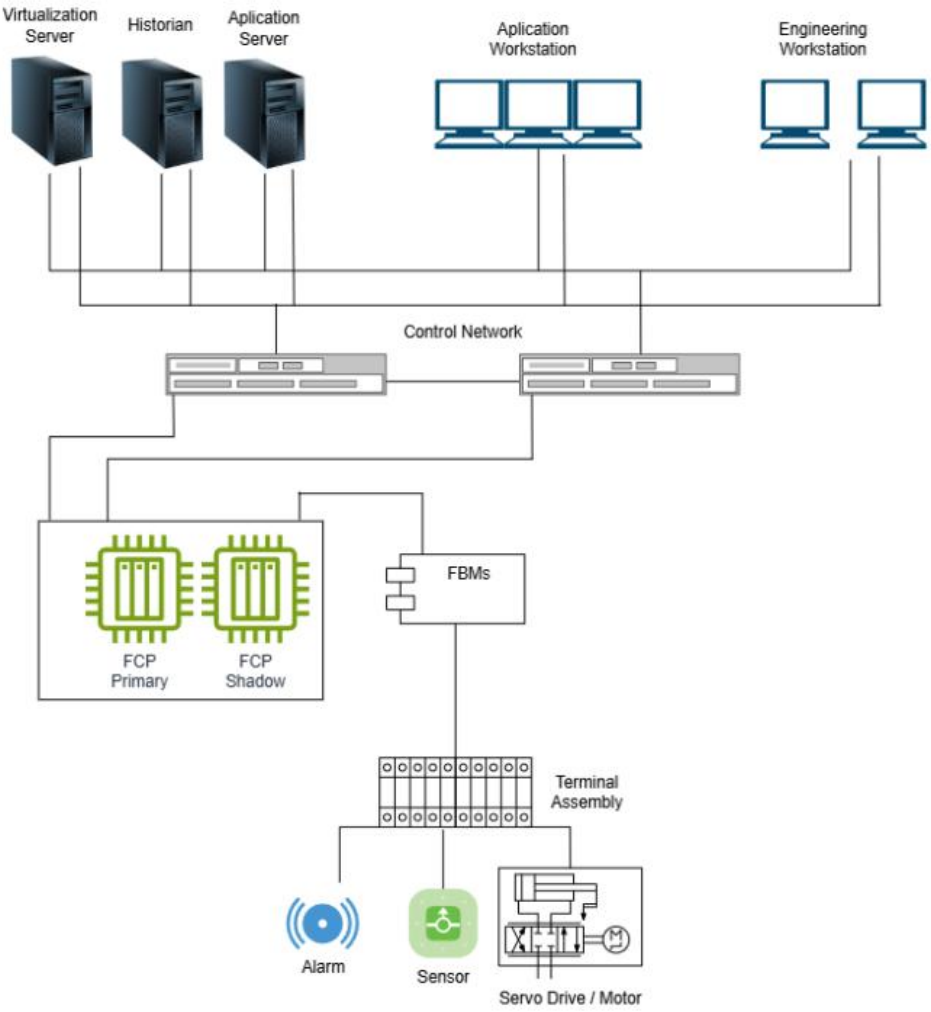
Nota. En la figura se muestra el diseño general del sistema SCADA.

DCS (Distributed Control System). Los DCS son sistemas de control diseñados para controlar procesos en una ubicación específica, como una planta de manufactura o

procesamiento. A diferencia de SCADA, los DCS se centran en controlar múltiples dispositivos y procesos de manera integrada en un área geográficamente delimitada. Esto permite una mayor precisión y confiabilidad en el control de procesos continuos. Sin embargo, los DCS pueden ser vulnerables a ataques internos que exploten el acceso a los sistemas de control en la planta, comprometiendo la operación y la seguridad (S. Khan & Madnick, 2021).

Figura 4

Ejemplo de una Implementación con DCS



Nota. En la figura se muestra un ejemplo de implementación con DCS.

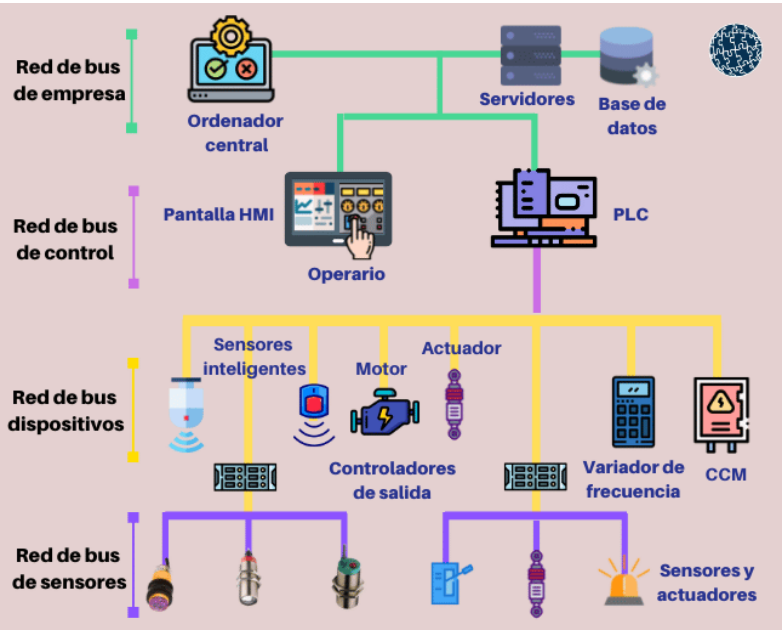
Redes de control industrial (Industrial Control Networks, ICN): son infraestructuras de comunicación diseñadas para conectar y coordinar dispositivos en entornos industriales, como

fábricas, plantas de energía y sistemas de automatización. Estas redes permiten la interacción entre sistemas de control, como SCADA, DCS y PLC, facilitando el monitoreo y la operación eficiente de procesos críticos en tiempo real (Conti et al., 2021).

A diferencia de las redes empresariales tradicionales, las ICN priorizan la confiabilidad, la disponibilidad y la baja latencia, utilizando protocolos especializados como Modbus, Profibus, EtherNet/IP y OPC UA. Sin embargo, con la creciente integración entre tecnologías de información (IT) y operación (OT), estas redes enfrentan desafíos significativos en ciberseguridad, debido a su dependencia de sistemas heredados y la falta de cifrado en muchos de sus protocolos, lo que las hace vulnerables a ataques cibernéticos. Por eso la importancia de implementar estrategias de protección como segmentación de redes, monitoreo continuo y actualización de sistemas para garantizar su seguridad y operatividad.

Figura 5

Niveles de bus de campo



Nota. En la figura se muestra los niveles de bus de campo. sicma21. Tomado de https://www.sicma21.com/bus-de-campo-aplicaciones-en-la-industria/.

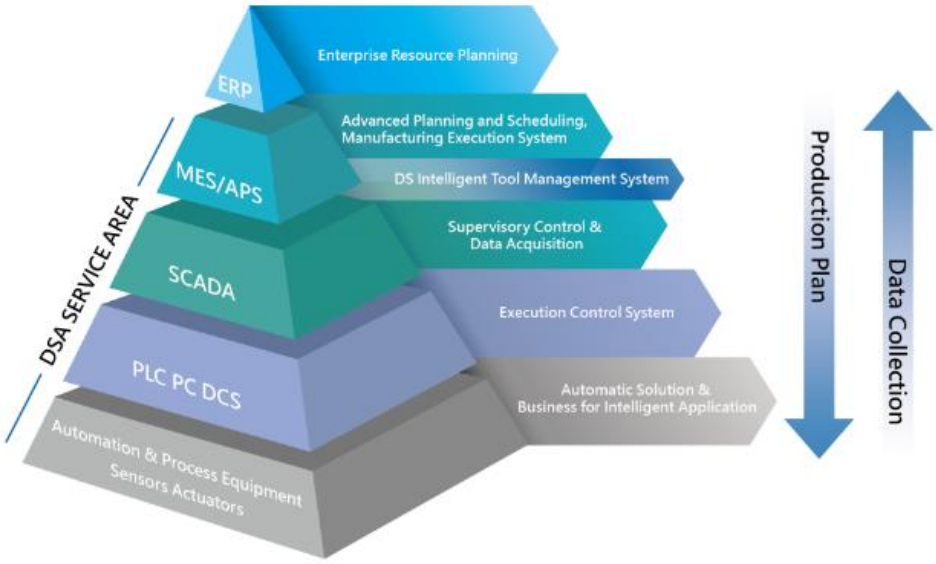
Pirámide CIM (Computer Integrated Manufacturing)

Es un modelo jerárquico que representa la estructura de automatización en la manufactura, dividiéndose en diferentes niveles según su función. Dentro de esta pirámide, los niveles de control y supervisión juegan un papel importante en la gestión eficiente de los procesos industriales. El nivel de control está compuesto por dispositivos como PLC (Controladores Lógicos Programables), que ejecutan tareas en tiempo real, como la activación de actuadores y la recopilación de datos de sensores.

Este nivel garantiza la correcta operación de la maquinaria y la producción. Por encima de este, el nivel de supervisión está representado por los sistemas SCADA (Supervisory Control and Data Acquisition) y DCS (Distributed Control Systems), que permiten la supervisión remota y centralizada de los procesos, proporcionando interfaces gráficas para los operadores, alarmas y herramientas de análisis de datos.

Figura 6

Pirámide CIM



Nota. En la figura se muestra el Manufacturing Execution System. dsa-auto. Tomado de https://www.dsa-auto.com.tw/en/p3_ai-system.php.

Marco Teórico

La ciberseguridad aplicada a los sistemas de control industrial (ICS) es un campo de estudio importante dentro de la seguridad de infraestructuras críticas. Debido a la creciente digitalización y conectividad de estos sistemas, ha surgido una amplia gama de amenazas cibernéticas que pueden comprometer la integridad, disponibilidad y confidencialidad de los procesos industriales. El marco teórico de esta investigación se fundamenta en el análisis de vulnerabilidades emergentes en los ICS, así como en el diseño e implementación de estrategias efectivas de mitigación.

Los ICS presentan características únicas que los diferencian de los entornos tradicionales de TI, Khan & Madnick (2021) proponen un enfoque sistémico para la identificación de vulnerabilidades y la definición de medidas de mitigación, destacando la necesidad de adoptar metodologías estructuradas que contemplen el ciclo de vida completo de los sistemas industriales. Entre las estrategias clave identificadas por estos autores se encuentran la segmentación de redes, que permite aislar componentes críticos y minimizar el riesgo de propagación de amenazas y la gestión proactiva de parches de seguridad, enfocada en actualizar software y firmware para reducir la exposición a exploits conocidos.

Ocaka et al. (2022) analizan el panorama de amenazas cibernéticas que afectan a los sistemas de control y automatización industrial, enfatizando la importancia de protocolos de seguridad robustos adaptados a las particularidades de estos entornos. Su investigación resalta que los ataques dirigidos a ICS pueden involucrar desde exploits de vulnerabilidades en protocolos de comunicación (como Modbus o DNP3) hasta el uso de malware avanzado diseñado para interrumpir o manipular procesos industriales. En este sentido, la adopción de

estrategias de defensa en profundidad es importante para garantizar la resiliencia de estos sistemas.

Zanasi et al. (2022) introducen la aplicación del modelo Zero Trust en la ciberseguridad de los ICS, el cual se basa en el principio de "nunca confiar, siempre verificar". Este modelo implica la verificación continua de identidades y accesos dentro del sistema, asegurando que incluso los usuarios y dispositivos autorizados sean monitoreados de manera constante. La implementación de Zero Trust en ICS implica la integración de autenticación multifactor, control de acceso basado en roles y monitoreo continuo del tráfico para detectar y bloquear actividades sospechosas en tiempo real.

El análisis de estos enfoques teóricos permite comprender la complejidad del problema de la ciberseguridad en los ICS y la necesidad de combinar múltiples estrategias para abordar eficazmente las amenazas emergentes. La evolución de los sistemas industriales hacia arquitecturas interconectadas exige un replanteamiento de los modelos de seguridad tradicionales y la adopción de metodologías que garanticen la protección de estos entornos críticos.

Marco Legal

La ciberseguridad en los sistemas de control industrial (ICS) se ha vuelto muy importante debido a la digitalización de las infraestructuras críticas y el aumento de ciberataques dirigidos a estos entornos. Como respuesta a esta amenaza, han surgido diversas normativas y estándares internacionales diseñados para establecer requisitos de seguridad y mejores prácticas en la protección de los ICS.

Uno de los marcos regulatorios más importantes es la norma IEC 62443, la cual proporciona un conjunto de directrices diseñadas específicamente para la seguridad de los ICS en entornos industriales. Esta norma se ha convertido en un referente clave en la industria, ya que

abarca múltiples aspectos de la ciberseguridad, desde la gestión del riesgo hasta la implementación de controles técnicos para proteger las redes y dispositivos industriales. Wang et al. (2023) analizan cómo el diseño de arquitecturas de seguridad basadas en IEC 62443 permite garantizar una protección integral de los sistemas industriales, asegurando la resiliencia ante ataques cibernéticos y mitigando vulnerabilidades en la infraestructura crítica.

A pesar de los avances en materia regulatoria, la seguridad en los ICS aún enfrenta desafíos debido a la falta de normativas específicas en muchos países. Históricamente, los ICS no contaban con regulaciones estrictas en términos de ciberseguridad, ya que su diseño original priorizaba la continuidad operativa sobre la protección contra amenazas digitales (Mestre, 2018). Sin embargo, con el incremento de incidentes de seguridad en infraestructuras críticas, estándares como IEC 62443 han ido ganando reconocimiento a nivel global, estableciendo lineamientos claros para la protección de estos entornos.

Además de los estándares internacionales, algunas regulaciones locales han comenzado a exigir medidas específicas para proteger infraestructuras críticas contra ciberataques. En muchos países, la legislación en ciberseguridad industrial se ha visto fortalecida por normativas nacionales que obligan a empresas y operadores de infraestructura crítica a implementar protocolos de seguridad más estrictos. Estas regulaciones buscan garantizar la integridad, disponibilidad y confidencialidad de los sistemas industriales, estableciendo sanciones en caso de incumplimiento.

Pablo & Gómez (2024) proponen un modelo para la gestión integral de vulnerabilidades en los ICS, basado en normativas internacionales y buenas prácticas de ciberseguridad. Su propuesta destaca la importancia de una estrategia de protección que no solo cumpla con

regulaciones existentes, sino que también adopte un enfoque proactivo para la detección y mitigación de riesgos en entornos industriales.

Marco Contextual

El contexto actual de los sistemas de control industrial (ICS) está marcado por una transformación impulsada por la convergencia entre las tecnologías de la información (IT) y las tecnologías operativas (OT). Esta integración ha permitido una gestión más eficiente y automatizada de los procesos industriales, mejorando la productividad y reduciendo costos. Sin embargo, también ha introducido nuevas vulnerabilidades, ya que los ICS, que anteriormente operaban en entornos aislados, ahora están expuestos a amenazas cibernéticas debido a su conexión con redes corporativas y dispositivos IoT.

García Núñez (2024) analiza cómo la convergencia IT-OT ha ampliado la superficie de ataque en los ICS, ya que muchas infraestructuras industriales han incluido tecnologías digitales sin contar con los controles de seguridad adecuados. Esto ha generado un ecosistema en el que los ciberataques pueden propagarse desde redes IT a los sistemas OT, comprometiendo procesos críticos y afectando la continuidad operativa.

Los dispositivos IoT industriales, como sensores inteligentes y sistemas de monitoreo remoto, han optimizado la supervisión de procesos en sectores como la manufactura, la energía y la distribución de agua. No obstante, la falta de medidas de seguridad en estos dispositivos ha abierto nuevas brechas de vulnerabilidad que pueden ser explotadas por atacantes para acceder a redes críticas (Damayanthy et al., 2022).

Uno de los sectores más afectados por estas amenazas es la industria química y energética, donde los ICS juegan un papel importante en la operación de plantas de producción y distribución. Yuan et al. (2024) presentan una evaluación integral de los riesgos de seguridad en

los sistemas ciberfísicos industriales, destacando la necesidad de estrategias avanzadas para proteger infraestructuras críticas. En este tipo de entornos, un ciberataque no solo podría provocar interrupciones operativas, sino también consecuencias devastadoras como explosiones, fugas de productos químicos peligrosos o interrupciones en el suministro de energía.

El impacto de las amenazas cibernéticas en los ICS no se limita a daños tecnológicos o financieros, sino que también representa un riesgo significativo para la seguridad pública y el medio ambiente. Sectores críticos como la energía, el agua y la manufactura dependen en gran medida de estos sistemas y un ataque exitoso podría generar apagones masivos, alteraciones en el tratamiento de agua potable o interrupciones en la producción de bienes esenciales.

En este contexto, resulta importante adoptar un enfoque de ciberseguridad proactivo, que combine tecnologías de detección y prevención de amenazas con estrategias de segmentación de redes, autenticación robusta y monitoreo continuo. A medida que los ICS continúan evolucionando hacia entornos interconectados, es imprescindible que las organizaciones industriales fortalezcan sus medidas de seguridad para mitigar los riesgos asociados a esta nueva realidad digital.

Diseño Metodológico

Tipo de Investigación

Este estudio se enmarca en un enfoque cualitativo exploratorio-descriptivo (Gauchi Risso, 2017), el cual permite comprender fenómenos como las vulnerabilidades emergentes en sistemas de control industrial, mediante el análisis de situaciones reales documentadas y el estudio detallado de fuentes especializadas. La investigación cualitativa resulta adecuada debido a que no se pretende cuantificar variables, sino entender el comportamiento de los sistemas, los

factores de riesgo y las estrategias de mitigación aplicadas o recomendadas en contextos específicos.

Selección de Casos de Estudio

Se seleccionaron cinco casos representativos de ataques cibernéticos contra ICS (Stuxnet, BlackEnergy, Triton, Colonial Pipeline y ataques a la industria del agua en EE. UU., 2021) debido a su alto impacto técnico, geopolítico y operacional, así como por la disponibilidad de documentación confiable. Estos casos fueron elegidos mediante un proceso de revisión documental, siguiendo criterios de inclusión como:

- Afectación directa a infraestructuras críticas que utilizan PLC, SCADA o DCS.
- Disponibilidad de análisis técnicos verificados por fuentes académicas o expertos del sector.
- Pertinencia frente a los objetivos específicos de esta investigación.

Como criterios de exclusión, se descartaron casos poco documentados, con fuentes no verificables o cuya naturaleza estuviese más orientada a ataques a tecnologías IT puras sin involucrar componentes ICS.

Recolección de datos

Se emplearon las siguientes técnicas:

Revisión documental. Se realizó una búsqueda sistemática en bases de datos académicas (IEEE Xplore, Scopus, ScienceDirect), portales especializados en ciberseguridad industrial (Dragos, CVE, NVD, American's Cyber Defence Agency) y estándares internacionales (NIST SP 800-82, IEC 62443).

Estudio de Casos. Se analizaron incidentes de ciberseguridad que ilustran las consecuencias de vulnerabilidades en sistemas industriales, destacando los vectores de ataque, el impacto y las respuestas implementadas.

Análisis Comparativo. Se compararon las estrategias de mitigación existentes con las amenazas actuales para identificar brechas de seguridad y proponer medidas adecuadas.

Herramientas y Técnicas de Análisis

Para el tratamiento y análisis de la información se aplicaron:

Análisis de Contenido. Para identificar patrones, riesgos recurrentes y debilidades comunes en los sistemas ICS.

Síntesis Temática. Agrupando hallazgos por tipo de sistema (PLC, SCADA, DCS, redes industriales) y por tipo de vulnerabilidad.

Categorización de Amenazas y Contramedidas. Basada en los lineamientos del NIST SP 800-82 y la norma IEC 62443.

Criterios de Calidad y Rigurosidad

- Se priorizaron fuentes confiables y verificadas, incluyendo estándares internacionales, investigaciones científicas y reportes técnicos con respaldo institucional.
- Se aplicó un enfoque crítico y sistemático para evaluar la solidez de las evidencias y su aplicabilidad en entornos reales.
- Se aseguró la coherencia metodológica entre los objetivos, la estrategia de recolección de datos y el tipo de análisis efectuado.

Identificación de las Vulnerabilidades en los Sistemas de Control Industrial

Los sistemas de control industrial son componentes críticos en la gestión y automatización de procesos dentro de sectores estratégicos como la energía, el transporte, la manufactura y la infraestructura crítica. Su función principal es garantizar la operación eficiente, segura y continua de estos entornos. Sin embargo, la creciente interconexión de estos sistemas con redes de Tecnología de la Información (IT) ha generado un escenario de riesgos sin precedentes, exponiendo vulnerabilidades que pueden ser explotadas por actores maliciosos con consecuencias potencialmente catastróficas (Weiss et al., 2022).

En este contexto, es importante identificar y comprender las principales vulnerabilidades asociadas a los componentes clave de los ICS, como los Controladores Lógicos Programables (PLC), los Sistemas de Control de Supervisión y Adquisición de Datos (SCADA) y los Sistemas de Control Distribuido (DCS). Estos dispositivos, aunque esenciales para la operación industrial, presentan debilidades que pueden ser aprovechadas para comprometer la seguridad y estabilidad de los procesos. Además, la convergencia entre las Tecnologías de la Información (IT) y las Tecnologías Operacionales (OT) ha introducido nuevas amenazas, ampliando la superficie de ataque y complicando los esfuerzos para garantizar la protección de estos sistemas (Mesbah et al., 2023).

La interconexión de redes IT y OT, aunque ofrece beneficios en términos de eficiencia y monitorización, también expone los ICS a amenazas tradicionales de ciberseguridad, como ataques de denegación de servicio (DoS), interceptación de comunicaciones (sniffing) y suplantación de identidad (spoofing). Esta convergencia ha transformado los entornos industriales en objetivos atractivos para ciberataques, lo que subraya la necesidad de implementar medidas de seguridad adaptadas a las particularidades de los ICS.

Estadísticas y Contexto

Según el programa CVE (Common Vulnerabilities and Exposures) gestionado por MITRE, hasta el año 2024 se han reportado más de 3.000 vulnerabilidades específicas asociadas a sistemas SCADA e ICS, con un crecimiento sostenido año tras año desde 2010 (CVE, 2025). Por su parte, la Base Nacional de Datos de Vulnerabilidades (NVD) del NIST proporciona un panorama detallado del impacto y severidad de estas vulnerabilidades, usando el sistema de puntuación CVSS, donde más del 51.4 % de los reportes sobre sistemas SCADA tienen una calificación superior a 7, indicando un riesgo alto o crítico para infraestructuras industriales (NIST, 2025).

Adicionalmente, la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) publica de forma periódica avisos (ICS Advisories) sobre vulnerabilidades en dispositivos específicos. En 2023, CISA emitió 392 alertas críticas relacionadas con ICS, de las cuales una gran proporción afectaba controladores PLC y plataformas SCADA utilizadas en sectores como energía, agua, transporte y manufactura (American´s Cyber Defence Agency, 2025).

Estudios como “The Global State of Security in Industrial Control Systems” revelan que más de 13.000 dispositivos ICS accesibles desde internet presentan al menos una vulnerabilidad crítica. Además, se identificó que los países con mayor exposición a sistemas vulnerables incluyen Estados Unidos, Alemania, Reino Unido, Brasil y Canadá, muchos de los cuales no cuentan con segmentación de red ni autenticación robusta(Anton et al., 2021). La presencia de dispositivos OT mal configurados en internet, visibles a través de herramientas como Shodan, representa un riesgo creciente para las infraestructuras críticas a nivel mundial.

Según el informe de Dragos de 2025, los ataques de ransomware contra organizaciones industriales aumentaron un 87 % respecto al año anterior, siendo el sector manufacturero el más

afectado, con un 71 % de los incidentes registrados. Este incremento se atribuye en parte a la explotación de vulnerabilidades en dispositivos PLC, como los modelos Unistream y Vision de Unitronics, que fueron comprometidos por el grupo hacktivista Hunt3r Kill3rs, afectando instalaciones en Europa y Estados Unidos, incluyendo plantas de energía renovable y estaciones de tratamiento de agua (Dragos, 2025).

En el informe de 2022, Dragos identificó un total de 2.170 vulnerabilidades en entornos ICS/OT, lo que representa un aumento del 46 % en comparación con años anteriores. Además, se destacó que el 80 % de las vulnerabilidades residían en lo profundo de las redes ICS y que el 53 % de las evaluaciones de servicios de Dragos revelaron problemas relacionados con la segmentación de redes. Estos hallazgos subrayan la necesidad de mejorar la visibilidad y el control de las conexiones en los entornos OT para mitigar los riesgos asociados (Dragos, 2023).

A continuación, se profundiza en las vulnerabilidades más comunes de estos sistemas y se analizan sus implicaciones para la seguridad industrial.

Vulnerabilidades en los PLC

Los controladores lógicos programables son los dispositivos encargados de la automatización y el control de procesos industriales. Estos equipos, diseñados para operar en entornos industriales exigentes, son responsables de ejecutar tareas críticas como la supervisión de maquinaria, la gestión de líneas de producción, el control de sistemas de energía y la regulación de procesos químicos. Su capacidad para operar en tiempo real y su flexibilidad para adaptarse a diferentes aplicaciones los convierten en un componente esencial en sectores como la manufactura, la energía, el transporte y la gestión de infraestructuras críticas.

Figura 7

PLC Modicon M580.

Nota. En la figura se muestra una PLC. Schneider Electric. Tomado de https://www.se.com/myschneider/catalogBrowse/co/es/product/BMEP585040C.

Sin embargo, a pesar de su importancia, los PLC presentan una serie de vulnerabilidades que pueden ser explotadas por actores maliciosos, comprometiendo no solo la seguridad de los sistemas, sino también la estabilidad y continuidad de los procesos industriales.

Un ataque exitoso contra un PLC podría resultar en la interrupción de operaciones críticas, daños físicos a equipos, pérdidas económicas significativas e incluso riesgos para la seguridad de las personas. A continuación, se profundiza en las principales debilidades de estos sistemas, analizando sus causas, implicaciones y posibles soluciones.

Falta de Autenticación y Control de Acceso

Los mecanismos de autenticación y control de acceso permiten proteger los PLC contra accesos no autorizados. Sin embargo, muchas implementaciones actuales presentan debilidades significativas que facilitan la explotación por parte de atacantes, algunas de las falencias en autenticación y control de acceso son:

Contraseñas predeterminadas y débiles: muchos fabricantes configuran los PLC con credenciales por defecto, como "admin/admin" o "1234", que rara vez son modificadas por los usuarios finales. Estas contraseñas, al ser ampliamente conocidas, pueden ser explotadas fácilmente por atacantes para obtener acceso no autorizado (Cusimano, 2022).Además, algunos modelos de PLC ni siquiera permiten establecer contraseñas, lo que deja el acceso completamente abierto a cualquier persona con conexión a la red.

Ausencia de autenticación multiusuario: en la mayoría de los entornos industriales, los PLC no cuentan con sistemas de autenticación robustos que permitan diferenciar entre usuarios con distintos niveles de acceso. Esto significa que cualquier persona con acceso a la red puede modificar configuraciones, cargar programas o alterar la lógica de control sin necesidad de credenciales adicionales. Esta falta de control facilita tanto ataques internos (por parte de empleados malintencionados) como externos (por parte de ciberdelincuentes).

Gestión inadecuada de privilegios: en numerosos casos, los PLC no permiten segmentar niveles de acceso, lo que significa que un operador con permisos básicos podría realizar cambios críticos en la programación del dispositivo. Esta falta de granularidad en los privilegios puede ocasionar fallos en la producción, interrupciones graves e incluso daños físicos a los equipos.

Protocolos de Comunicación Inseguros

La seguridad en las comunicaciones es otro aspecto crítico en los PLC, dado que muchos de estos dispositivos operan con protocolos propietarios o antiguos que carecen de mecanismos de protección adecuados.

Uso de protocolos sin cifrado: muchos PLC utilizan protocolos como Modbus, DNP3 y PROFINET, los cuales transmiten información en texto claro sin mecanismos de cifrado. Esto permite a los atacantes interceptar y modificar paquetes de datos a través de ataques de man-in-the-middle (MITM), comprometiendo la integridad y confidencialidad de las comunicaciones.

Falta de mecanismos de integridad: la mayoría de los protocolos utilizados por los PLC no incluyen mecanismos de verificación de integridad de los datos, lo que hace posible la manipulación de comandos sin que el sistema detecte la alteración. Por ejemplo, un atacante podría modificar un comando para detener una línea de producción o alterar parámetros críticos, como la temperatura o presión en un proceso industrial.

Riesgos en la convergencia IT-OT: con la creciente integración entre las Tecnologías de la Información (IT) y las Tecnologías Operacionales (OT), los PLC quedan expuestos a redes IP que pueden ser objetivo de ataques tradicionales como denegación de servicio (DoS), sniffing y spoofing. Esta convergencia amplía la superficie de ataque y complica los esfuerzos para garantizar la seguridad de los sistemas (Pal et al., 2023).

Explotación de Vulnerabilidades en Firmware

El firmware de los PLC representa otro punto vulnerable, ya que los atacantes pueden explotarlo de diferentes maneras para comprometer la seguridad de los sistemas.

Falta de actualizaciones y parches de seguridad: muchos PLC operan con firmware obsoleto que contiene vulnerabilidades conocidas, pero no pueden ser actualizados fácilmente debido a restricciones en la infraestructura industrial o incompatibilidades con software

heredado. Esto deja los sistemas expuestos a ataques que explotan vulnerabilidades ya parcheadas en versiones más recientes.

Ataques mediante ingeniería inversa: los atacantes pueden analizar el firmware de un PLC en busca de vulnerabilidades no documentadas que permitan la ejecución de código malicioso o la toma de control del dispositivo. Este tipo de ataques es particularmente peligroso, ya que puede permitir a los atacantes modificar la lógica de control sin ser detectados.

Carga de firmware malicioso: algunos PLC permiten la actualización de firmware sin validación criptográfica, lo que posibilita que un atacante suba versiones modificadas para introducir puertas traseras (backdoors) o modificar la lógica de control. Esto podría resultar en la interrupción de procesos críticos o incluso en daños físicos a los equipos (Hollerer et al., 2022).

Las vulnerabilidades en los PLC representan un riesgo significativo para la seguridad de los sistemas de control industrial ICS. La falta de autenticación robusta, el uso de protocolos de comunicación inseguros y la explotación de vulnerabilidades en el firmware son solo algunas de las debilidades que pueden ser explotadas por atacantes para comprometer la operación de infraestructuras críticas.

Tabla 1

Resumen de Vulnerabilidades en los PLCs

Vulnerabilidad	Descripción
Contraseñas predeterminadas y débiles	Uso de credenciales por defecto que rara vez son modificadas, facilitando accesos no autorizados.
Ausencia de autenticación multiusuario	Falta de control granular de acceso, permitiendo que cualquier usuario en la red pueda modificar la configuración del PLC.
Gestión inadecuada de privilegios	Falta de segmentación de accesos, permitiendo a usuarios no autorizados modificar parámetros críticos.
Uso de protocolos sin cifrado	Uso de Modbus, DNP3, PROFINET sin cifrado, permitiendo interceptación y manipulación de datos.
Falta de mecanismos de integridad	No se verifica la integridad de los datos transmitidos, permitiendo modificaciones sin ser detectadas.
Riesgos en la convergencia IT-OT	Integración de redes industriales con redes IT tradicionales, aumentando la superficie de ataque.

Vulnerabilidad	Descripción
Falta de actualizaciones y parches de seguridad	Uso de firmware obsoleto con vulnerabilidades conocidas sin parches disponibles.
Ataques mediante ingeniería inversa	Análisis del firmware en busca de vulnerabilidades explotables por atacantes.
Carga de firmware malicioso	Posibilidad de cargar firmware no autenticado, introduciendo puertas traseras y código malicioso.

Nota. En la tabla se realiza un resumen de vulnerabilidades en los PLCs.

Vulnerabilidades en los sistemas SCADA

Los sistemas SCADA (Supervisory Control and Data Acquisition, por sus siglas en inglés) permiten la gestión y operación de infraestructuras críticas y procesos industriales complejos. Estos sistemas se utilizan ampliamente en sectores como la generación y distribución de energía eléctrica, plantas de tratamiento de agua y aguas residuales, sistemas de transporte, refinerías, fábricas de manufactura y otras industrias donde la supervisión y el control en tiempo real son esenciales. Su función principal es recopilar datos de campo a través de sensores y dispositivos de control, procesar esta información en una interfaz centralizada y permitir la toma de decisiones automatizada o manual para optimizar los procesos.

Los sistemas SCADA permiten la automatización de tareas, el monitoreo remoto de operaciones y la gestión eficiente de recursos, lo que los convierte en un componente indispensable para garantizar la continuidad y seguridad de los servicios públicos y las operaciones industriales. Por ejemplo, en una red eléctrica, un sistema SCADA puede supervisar el flujo de energía, detectar fallas en la red y activar mecanismos de protección para evitar cortes masivos. En una planta de tratamiento de agua, puede monitorear los niveles de calidad del agua y controlar las bombas y válvulas para garantizar un suministro seguro y constante.

Sin embargo, a pesar de su importancia, los sistemas SCADA enfrentan desafíos significativos en términos de seguridad cibernética. Su naturaleza distribuida, que implica la

conexión de múltiples dispositivos (como sensores, actuadores, PLC y servidores) a través de redes locales o remotas, los hace vulnerables a una amplia gama de amenazas. Además, la creciente convergencia entre las Tecnologías de la Información (IT) y las Tecnologías Operacionales (OT) ha expuesto estos sistemas a riesgos que antes eran más comunes en entornos corporativos, como ataques de ransomware, denegación de servicio (DoS) y explotación de vulnerabilidades en software y hardware (Quiroz Tascón et al., 2020).

Estas vulnerabilidades no solo ponen en riesgo la seguridad operativa de las infraestructuras críticas, sino que también amenazan la disponibilidad de servicios esenciales para las personas. Un ataque exitoso contra un sistema SCADA podría resultar en cortes de energía, contaminación del suministro de agua, interrupciones en el transporte o incluso daños físicos a equipos y personas. Por ejemplo, el famoso ataque a la red eléctrica de Ucrania en 2015, conocido como BlackEnergy, demostró cómo los ciberataques pueden causar apagones masivos y afectar a cientos de miles de personas (Duo et al., 2022).

Figura 8

Sistema SCADA.

Nota. En la figura se muestra un ejemplo de SCADA. Intellymation. Tomado de https://intellymation.com.ar/diferencias-scada-hmi/

Algunas de las vulnerabilidades más significativas incluyen:

Dependencia de Sistemas Operativos Obsoletos

Uno de los problemas más críticos en los sistemas SCADA es su dependencia de versiones antiguas de sistemas operativos, como Windows XP o Windows 7, los cuales han alcanzado su fin de vida útil y ya no reciben actualizaciones de seguridad por parte de los fabricantes. Esta falta de soporte deja expuestos a estos sistemas a exploits ampliamente documentados que pueden ser aprovechados por atacantes para ejecutar código malicioso de manera remota o escalar privilegios dentro del sistema (Mesbah et al., 2023).

Además, debido a que muchos sistemas SCADA requieren estabilidad y compatibilidad con aplicaciones heredadas, la migración a sistemas operativos modernos suele ser un proceso complejo y costoso. En algunos casos, la actualización de un solo componente puede generar problemas de interoperabilidad con hardware y software especializado, lo que lleva a que muchas organizaciones continúen utilizando sistemas vulnerables.

Ejemplos de ataques reales demuestran la gravedad de esta problemática. El ataque de ransomware WannaCry en 2017 afectó a múltiples organizaciones que ejecutaban versiones sin parchear de Windows, incluyendo sistemas industriales, lo que interrumpió la operación de hospitales, fábricas y redes de transporte.

Falta de Segmentación ede Red

La falta de segmentación de red es una de las vulnerabilidades más críticas en los entornos industriales, especialmente en sistemas SCADA. Cuando no existe una separación adecuada entre la red SCADA y otras redes corporativas o administrativas, la superficie de ataque se incrementa significativamente. En muchos casos, los sistemas SCADA están conectados directamente a redes menos seguras, como las redes de oficina o incluso a internet,

sin los controles de seguridad adecuados. Esto permite que los atacantes exploten vulnerabilidades en sistemas menos críticos, como servidores de correo o estaciones de trabajo, para luego acceder a los sistemas de control industrial (Ryu et al., 2024). La ausencia de barreras claras entre estas redes facilita el movimiento lateral de los atacantes, poniendo en riesgo la operación de infraestructuras críticas.

El movimiento lateral es una técnica utilizada por los ciberdelincuentes para desplazarse dentro de una red una vez que han obtenido acceso inicial. En entornos industriales, esta técnica es particularmente peligrosa porque los atacantes pueden pasar de sistemas no críticos, como computadoras de oficina, a sistemas críticos, como los SCADA, sin ser detectados. Un ejemplo emblemático de este tipo de ataque es el incidente de 2015 en la red eléctrica de Ucrania, donde los atacantes utilizaron correos electrónicos de phishing para comprometer la red administrativa (R. Khan et al., 2016). Una vez dentro, se movieron lateralmente hasta alcanzar los sistemas SCADA, desde donde causaron apagones masivos que afectaron a cientos de miles de personas. Este caso demostró cómo la falta de segmentación puede tener consecuencias devastadoras en infraestructuras críticas.

La convergencia entre las redes IT y OT ha profundizado este problema. A medida que los sistemas industriales se integran con redes corporativas para mejorar la eficiencia y el monitoreo, también se vuelven más vulnerables a amenazas tradicionales de IT, como ransomware, malware y ataques de denegación de servicio (DoS). Sin una segmentación adecuada, un ataque dirigido a la red corporativa puede propagarse fácilmente a los sistemas de control industrial, interrumpiendo operaciones críticas y causando daños económicos y reputacionales significativos. Por ejemplo, un ataque de ransomware en una red administrativa

podría extenderse a los sistemas SCADA, paralizando la producción y obligando a las empresas a detener sus operaciones.

La falta de segmentación de red es una vulnerabilidad crítica que expone a los sistemas SCADA y otros componentes industriales a ciberataques. La implementación de una arquitectura de red segmentada no solo reduce la superficie de ataque, sino que también limita el impacto de posibles brechas de seguridad.

Configuraciones Predeterminadas Inseguras

Las configuraciones predeterminadas inseguras en los sistemas SCADA representan una de las principales vulnerabilidades en la seguridad de infraestructuras críticas. Estos dispositivos y software suelen venir configurados con parámetros estándar que no están diseñados para resistir ataques cibernéticos, lo que facilita la explotación de sus debilidades. Entre los problemas más comunes se encuentran el uso de credenciales por defecto, la falta de cifrado en los protocolos de comunicación y el acceso remoto sin medidas de autenticación robustas. Estas fallas pueden ser aprovechadas por actores malintencionados para comprometer la operación de sistemas industriales esenciales.

El uso de credenciales por defecto es una de las fallas más recurrentes en los sistemas SCADA. Muchos dispositivos vienen configurados con nombres de usuario y contraseñas predefinidas, como "admin/admin" o "1234", lo que facilita su acceso no autorizado. Los atacantes pueden explotar esta vulnerabilidad mediante ataques de fuerza bruta o utilizando bases de datos de credenciales filtradas. Si estas credenciales no son cambiadas tras la instalación, cualquier persona con conocimientos básicos de ciberseguridad podría obtener acceso al sistema, poniendo en riesgo la integridad y disponibilidad de los procesos industriales.

Otra de las configuraciones inseguras comunes es el uso de protocolos de comunicación sin cifrado, como Modbus, DNP3 o BACnet. Estos protocolos transmiten información en texto plano, permitiendo que atacantes intercepten y manipulen los datos sin dificultad (Zare et al., 2024). En un escenario de ataque dirigido, un adversario podría modificar comandos críticos, como la apertura de válvulas en una planta de tratamiento de agua o la alteración de parámetros en una línea de producción. La falta de cifrado en la transmisión de datos expone a los sistemas SCADA a ataques de interceptación y manipulación, comprometiendo la seguridad y estabilidad de los procesos industriales.

El acceso remoto no seguro es otro riesgo significativo en los sistemas SCADA. Muchas configuraciones predeterminadas permiten conexiones remotas sin autenticación adecuada, lo que facilita accesos no autorizados desde cualquier dirección IP. Existen casos documentados en los que sistemas SCADA han sido encontrados accesibles en internet a través de motores de búsqueda especializados como Shodan. Esta exposición pública deja a las infraestructuras críticas vulnerables a ataques remotos, que pueden ir desde la manipulación de procesos hasta la interrupción total de operaciones.

Las configuraciones predeterminadas inseguras en los sistemas SCADA representan un riesgo grave para la seguridad de las infraestructuras industriales. La combinación de credenciales por defecto, protocolos sin cifrado y acceso remoto sin protección adecuada facilita la explotación de vulnerabilidades por parte de atacantes.

Tabla 2

Resumen de las Vulnerabilidades en los SCADA

Vulnerabilidad	Descripción
Dependencia de sistemas operativos obsoletos	Uso de versiones antiguas de Windows (XP, 7) sin actualizaciones de seguridad.
Falta de segmentación de red	Conexión directa de sistemas SCADA con redes corporativas o internet sin separación adecuada.
Configuraciones predeterminadas inseguras	Uso de credenciales por defecto, protocolos sin cifrado y acceso remoto sin autenticación segura.

Nota. En la tabla se realiza un resumen de las vulnerabilidades en los SCADA.

Vulnerabilidades en los Sistemas DCS

Los sistemas de control distribuido son una arquitectura de control utilizada en entornos industriales para supervisar y gestionar procesos automatizados de manera eficiente. A diferencia de los sistemas de control centralizados, un DCS se compone de múltiples controladores distribuidos en distintas ubicaciones dentro de una planta o instalación industrial. Estos controladores trabajan de manera coordinada y están conectados a través de una red de comunicación, lo que permite mejorar la confiabilidad y la capacidad de respuesta del sistema ante cambios en las condiciones operativas (Cusimano, 2022).

Una de las principales ventajas de un DCS es su capacidad para operar en tiempo real, lo que facilita la toma de decisiones automatizadas sin la necesidad de intervención humana constante. Esto es particularmente útil en sectores como la manufactura, la producción de energía, la industria química y el tratamiento de agua, donde la precisión y la continuidad operativa son esenciales. Además, los DCS suelen integrar interfaces hombre-máquina (HMI) que permiten a los operadores monitorear y ajustar parámetros del sistema en tiempo real.

Sin embargo, la creciente interconexión de los DCS con redes empresariales y sistemas de TI ha generado nuevas vulnerabilidades de ciberseguridad. Muchos DCS utilizan protocolos

de comunicación heredados y carecen de mecanismos robustos de autenticación y cifrado, lo que los hace susceptibles a ataques como la interceptación de datos, la manipulación de procesos y el acceso no autorizado. Además, la dependencia de sistemas operativos obsoletos y la falta de segmentación de red pueden aumentar el riesgo de amenazas como el ransomware y los ataques dirigidos a infraestructuras críticas (Weiss et al., 2022).

Sistemas Operativos Obsoletos

Los sistemas operativos obsoletos representan una de las principales vulnerabilidades en los DCS debido a la falta de actualizaciones de seguridad y soporte técnico por parte de los fabricantes. Muchos DCS operan sobre versiones antiguas de Windows, como Windows XP o Windows 7, que ya no reciben parches de seguridad. Esto significa que cualquier vulnerabilidad descubierta en estos sistemas queda permanentemente expuesta, permitiendo que los atacantes exploten fallos conocidos para obtener acceso no autorizado, ejecutar código malicioso o incluso tomar el control de los procesos industriales (Andreeva et al., 2016).

Además de la ausencia de actualizaciones, los sistemas operativos obsoletos son incompatibles con muchas soluciones modernas de ciberseguridad. Herramientas como antivirus avanzados, sistemas de detección y prevención de intrusiones (IDS/IPS) y software de monitoreo en tiempo real suelen requerir versiones más recientes del sistema operativo para su correcto funcionamiento. Como resultado, los DCS que dependen de sistemas operativos antiguos quedan sin una capa de defensa adecuada, lo que los convierte en objetivos fáciles para ataques cibernéticos sofisticados.

Otro problema significativo es la exposición de los DCS a ataques de ransomware y malware específicamente diseñados para explotar vulnerabilidades en sistemas sin soporte. Un caso emblemático es el ataque de ransomware WannaCry en 2017, que afectó miles de sistemas

en todo el mundo al aprovechar una vulnerabilidad en versiones obsoletas de Windows. En un entorno industrial, un ataque de este tipo podría paralizar operaciones críticas, causando interrupciones en la producción, pérdidas económicas significativas y riesgos para la seguridad física de los trabajadores y las instalaciones (Benmalek, 2024).

La migración a versiones más recientes de sistemas operativos en entornos industriales no siempre es sencilla debido a la compatibilidad con software y hardware heredado. Muchos DCS fueron diseñados para operar exclusivamente con versiones específicas de sistemas operativos y actualizar estos componentes puede requerir una inversión considerable en tiempo y recursos. Sin embargo, mantener estos sistemas sin actualizaciones de seguridad es un riesgo, por lo que las organizaciones deben evaluar estrategias como la virtualización, la segmentación de red y el endurecimiento del sistema para mitigar las amenazas asociadas a sistemas operativos obsoletos.

La presencia de sistemas operativos desactualizados en los DCS representa una vulnerabilidad crítica que puede ser explotada por atacantes para comprometer infraestructuras industriales. La falta de parches de seguridad, la incompatibilidad con soluciones modernas de ciberseguridad y la exposición a amenazas como el ransomware hacen imperativo que las organizaciones implementen estrategias de mitigación.

Conectividad Insegura y Falta de Segmentación de Red

La conectividad insegura y la falta de segmentación de red en los DCS representan vulnerabilidades críticas que pueden ser explotadas por atacantes para comprometer la integridad, disponibilidad y confidencialidad de los procesos industriales. En muchos casos, los DCS están conectados directamente a la red corporativa o incluso a Internet sin las medidas de seguridad adecuadas, lo que amplía la superficie de ataque y facilita accesos no autorizados. Esta exposición es particularmente peligrosa cuando los sistemas carecen de controles de acceso

robustos, lo que permite a ciberdelincuentes infiltrarse y manipular los procesos de automatización industrial (Djebbar & Nordstrom, 2023).

Uno de los principales riesgos de la conectividad insegura es el acceso remoto sin restricciones ni mecanismos de autenticación fuertes. Muchos sistemas DCS permiten conexiones remotas para la supervisión y el mantenimiento, pero sin una configuración adecuada, estas conexiones pueden ser aprovechadas por atacantes para ingresar a la red. Sin una segmentación de red efectiva, un atacante que acceda remotamente podría moverse lateralmente dentro de la infraestructura y comprometer múltiples dispositivos.

La falta de segmentación de red es otro problema crítico en los DCS, ya que permite que los sistemas de control industrial coexistan en la misma red que los sistemas corporativos, exponiéndolos a amenazas provenientes de dispositivos menos seguros. Si un equipo en la red empresarial se ve comprometido por malware o ransomware, este puede propagarse fácilmente a los sistemas DCS, afectando su operación.

Otro aspecto de la conectividad insegura es el uso de protocolos de comunicación sin cifrado, como Modbus, DNP3 y BACnet, que transmiten datos en texto plano sin ningún tipo de protección. Esto permite a los atacantes interceptar, modificar o inyectar comandos maliciosos en la red de control, alterando el comportamiento de los procesos industriales.

La conectividad insegura y la falta de segmentación de red en los DCS representan vulnerabilidades que pueden ser explotadas para comprometer infraestructuras industriales. La implementación de controles de acceso estrictos, el uso de redes segregadas para los sistemas de control, la adopción de protocolos de comunicación cifrados y el monitoreo continuo del tráfico de red son medidas para reducir el riesgo.

Protocolos de Comunicación sin Cifrado

Los protocolos de comunicación sin cifrado representan una vulnerabilidad crítica en los DCS debido a la falta de protección en la transmisión de datos entre dispositivos y componentes del sistema. Muchos protocolos industriales, como Modbus, DNP3 y BACnet, fueron diseñados en una época donde la ciberseguridad no era una preocupación primordial. Como resultado, estos protocolos transmiten datos en texto plano, sin ninguna forma de cifrado o autenticación, lo que los hace susceptibles a diversas amenazas cibernéticas, como la interceptación de datos y la manipulación de comandos (Alqudhaibi et al., 2023).

Uno de los principales riesgos de los protocolos sin cifrado es la posibilidad de ataques de interceptación o "man-in-the-middle" (MITM). En estos ataques, un ciberdelincuente puede capturar y leer el tráfico de red que circula entre los dispositivos de control y los sistemas de supervisión. Esto permite que el atacante obtenga información sensible sobre la operación del sistema, como comandos de control, valores de sensores y parámetros críticos de procesos industriales. Con esta información, un adversario podría comprender el funcionamiento interno del sistema y planear ataques más dirigidos y destructivos.

Además de la interceptación, los protocolos sin cifrado permiten la manipulación de datos, lo que puede tener consecuencias devastadoras para los procesos industriales. Un atacante que logra inyectar comandos maliciosos en la red puede modificar variables de control, alterar el funcionamiento de equipos o incluso detener la producción en una planta industrial. Por ejemplo, en una instalación de energía, un atacante podría enviar señales falsas para abrir o cerrar interruptores eléctricos, causando apagones o sobrecargas en el sistema. Este tipo de ataques pone en riesgo la integridad y disponibilidad de la infraestructura crítica.

Otro problema derivado del uso de protocolos sin cifrado es la dificultad para detectar ataques en tiempo real. Como no hay mecanismos de autenticación ni integridad en la

comunicación, un atacante puede modificar paquetes de datos sin que el sistema lo detecte inmediatamente. Esto puede dar lugar a ataques persistentes donde los ciberdelincuentes manipulan gradualmente las operaciones del DCS sin ser detectados. La ausencia de registros seguros y la falta de monitoreo avanzado dificultan la identificación temprana de actividades sospechosas.

Para mitigar esta vulnerabilidad, las organizaciones podrían adoptar medidas de seguridad como el uso de versiones seguras de estos protocolos, la implementación de túneles VPN cifrados para la comunicación remota y la aplicación de soluciones de monitoreo de tráfico de red. Además, se recomienda la segmentación de red para aislar los sistemas de control de redes externas y minimizar el riesgo de accesos no autorizados.

Configuraciones Predeterminadas Inseguras

Las configuraciones predeterminadas inseguras en los DCS representan una vulnerabilidad crítica, ya que muchas de estas configuraciones no están diseñadas para resistir ataques cibernéticos. Los dispositivos y software que conforman un DCS suelen venir preconfigurados con parámetros estándar que facilitan su instalación y operación, pero que, si no se modifican adecuadamente, pueden ser explotados por atacantes. Entre las configuraciones más problemáticas se encuentran las credenciales por defecto, la exposición innecesaria de servicios y la falta de mecanismos de autenticación y cifrado (Weiss et al., 2022).

Uno de los problemas más comunes es el uso de credenciales predeterminadas, como "admin/admin" o "1234", las cuales son ampliamente conocidas y utilizadas por los fabricantes. Si los operadores del sistema no cambian estas credenciales tras la instalación, los atacantes pueden obtener acceso fácilmente a los dispositivos y tomar control del sistema. Este tipo de fallos ha sido aprovechado en múltiples ataques a infraestructuras industriales, donde los

ciberdelincuentes han logrado comprometer sistemas críticos simplemente utilizando credenciales por defecto que no fueron modificadas.

Otro aspecto preocupante de las configuraciones predeterminadas inseguras es la exposición innecesaria de servicios y puertos. Muchos dispositivos DCS vienen configurados con servicios de administración remota habilitados por defecto, lo que permite accesos externos sin las debidas restricciones. Si estos servicios no son desactivados o protegidos con medidas de seguridad adecuadas, los atacantes pueden explotar vulnerabilidades en estos servicios para infiltrarse en la red de control. En algunos casos, sistemas DCS han sido encontrados accesibles a través de motores de búsqueda, exponiéndolos a ataques remotos.

Además, la falta de cifrado en las comunicaciones predeterminadas de muchos dispositivos DCS es una vulnerabilidad crítica. Algunos protocolos de comunicación industriales, como Modbus y DNP3, se configuran sin autenticación ni cifrado, permitiendo que cualquier actor malintencionado intercepte y manipule los datos que circulan por la red. Esto podría dar lugar a ataques donde los comandos enviados a los dispositivos de control sean alterados sin que los operadores lo detecten, poniendo en riesgo la seguridad de las operaciones industriales.

Para mitigar estas vulnerabilidades, se deben cambiar las credenciales por defecto inmediatamente después de la instalación, deshabilitar servicios innecesarios, aplicar autenticación robusta y cifrado en las comunicaciones y segmentar la red de control para minimizar la exposición a amenazas externas. Solo a través de una gestión proactiva de la seguridad en la configuración del DCS se puede reducir el riesgo de ataques y garantizar la continuidad operativa de los sistemas industriales.

Tabla 3

Resumen de las Vulnerabilidades en los DCS

Vulnerabilidad	Descripción
Sistemas operativos obsoletos	Uso de versiones antiguas de SO sin actualizaciones ni soporte, exponiéndolos a vulnerabilidades conocidas.
Conectividad insegura y falta de segmentación de red	Conexión directa de DCS a redes corporativas o Internet sin controles adecuados, facilitando accesos no autorizados.
Protocolos de comunicación sin cifrado	Uso de protocolos industriales antiguos que transmiten datos en texto plano sin autenticación ni cifrado.
Configuraciones predeterminadas inseguras	Uso de credenciales por defecto, permisos excesivos o configuración estándar sin endurecimiento de seguridad.
Falta de monitoreo y detección de intrusiones	Ausencia de herramientas de supervisión activa y detección de amenazas en tiempo real en los DCS.
Ingeniería social y phishing	Engaños a empleados para obtener credenciales o acceso a sistemas críticos.
Exposición de dispositivos a Internet	Dispositivos de control expuestos en redes públicas sin restricciones, facilitando accesos no autorizados.
Dependencia de software heredado	Uso de aplicaciones y herramientas antiguas que no pueden ser actualizadas sin afectar la operatividad del sistema.
Ataques físicos a la infraestructura	Acceso físico no autorizado a equipos de control, manipulación de hardware, instalación de dispositivos maliciosos.
Inyección de código malicioso en controladores	Explotación de vulnerabilidades en PLCs y dispositivos de control para ejecutar código malicioso.

Nota. En la tabla se realiza un resumen de vulnerabilidades en los DCS.

Vulnerabilidades en Redes de Control Industrial

Las redes de control industrial (ICN) desempeñan un papel crítico en la supervisión y operación de procesos industriales, pero presentan vulnerabilidades significativas que pueden comprometer su seguridad y disponibilidad. Una de las principales debilidades radica en el uso de protocolos de comunicación no seguros, como Modbus, DNP3 y Profibus, que fueron diseñados originalmente sin mecanismos de cifrado o autenticación. Esto permite que un atacante pueda interceptar, manipular o suplantar comandos en la red, generando interrupciones en los procesos o alterando el funcionamiento de los sistemas industriales. Además, muchas organizaciones no implementan controles adecuados para restringir el acceso a estos protocolos, dejando expuestos sus dispositivos a ataques remotos o internos.

Otra vulnerabilidad crítica es la obsolescencia tecnológica en los entornos industriales. Muchos sistemas de control operan con hardware y software heredados que no reciben actualizaciones de seguridad, lo que los convierte en objetivos fáciles para ataques cibernéticos. En algunos casos, los fabricantes han dejado de brindar soporte a estos dispositivos, impidiendo la aplicación de parches para corregir vulnerabilidades conocidas (Hollerer et al., 2022). Además, la dependencia de sistemas antiguos hace que la modernización sea un proceso complejo y costoso, lo que lleva a muchas empresas a postergar mejoras de seguridad y aumentar su exposición a amenazas.

La convergencia entre redes IT (Tecnología de la Información) y OT (Tecnología Operacional) ha aumentado la superficie de ataque de los sistemas industriales. La interconexión con redes corporativas permite una mayor eficiencia operativa, pero también introduce riesgos, ya que una brecha en la infraestructura de TI puede afectar directamente los sistemas de control industrial. Ataques como ransomware, accesos remotos no autorizados y malware especializado pueden propagarse desde la red corporativa a la red industrial, generando daños operativos significativos. Además, la falta de segmentación adecuada entre IT y OT permite que los atacantes se desplacen lateralmente dentro de la infraestructura, accediendo a dispositivos críticos sin restricciones adecuadas (Pancho & Galarza, 2014).

La falta de capacitación en ciberseguridad y errores humanos representan una amenaza constante en las redes de control industrial. Configuraciones incorrectas, contraseñas débiles o el desconocimiento de buenas prácticas de seguridad pueden facilitar accesos no autorizados y ataques internos o externos. La ausencia de políticas de gestión de accesos y monitoreo en tiempo real puede permitir que intrusos permanezcan en la red sin ser detectados, aumentando el riesgo de sabotaje o robo de información sensible.

Protocolos Inseguros

Las redes de control industrial dependen de protocolos de comunicación diseñados originalmente para operar en entornos cerrados, sin considerar la seguridad como un factor prioritario. Protocolos como Modbus, DNP3, BACnet y Profibus carecen de mecanismos de autenticación, cifrado o control de acceso, lo que los hace altamente vulnerables a ataques como la interceptación de datos (sniffing) y la manipulación de paquetes. Un atacante que tenga acceso a la red puede fácilmente modificar comandos, lo que podría causar fallos en la producción, interrupciones del servicio o daños a los equipos.

Además, muchos dispositivos industriales utilizan estos protocolos sin aplicar medidas de seguridad adicionales, como túneles VPN o cifrado TLS, lo que facilita los ataques de intermediario (Man-in-the-Middle, MitM). Un atacante podría alterar los datos de sensores o modificar comandos enviados a los actuadores sin ser detectado. Esta debilidad es especialmente crítica en sectores como la energía, la manufactura y el transporte, donde la alteración de parámetros de operación puede generar consecuencias catastróficas.

Otro problema radica en la falta de autenticación en la mayoría de estos protocolos. Cualquier actor malintencionado con acceso a la red puede enviar comandos a los dispositivos sin necesidad de credenciales, lo que permite la ejecución de ataques de control remoto. La ausencia de registros detallados de actividad en muchos sistemas dificulta la detección de accesos no autorizados, lo que agrava la situación.

Para mitigar estos riesgos, es importante adoptar medidas de seguridad como la implementación de firewalls industriales, el uso de VPNs para conexiones remotas seguras y la migración a protocolos más seguros como OPC UA, que ofrece autenticación y cifrado.

Puertos y Servicios Expuestos

La exposición de puertos y servicios innecesarios en dispositivos industriales representa una de las principales vulnerabilidades en las redes de control. Muchas veces, los sistemas de control se configuran con puertos abiertos para facilitar la administración remota o la integración con otros sistemas, sin considerar los riesgos de seguridad que esto implica. Un atacante que escanee la red puede identificar servicios activos y explotarlos para obtener acceso no autorizado.

Entre los puertos más comúnmente expuestos en redes industriales se encuentran 502/TCP (Modbus), 44818/TCP (EtherNet/IP), 2404/TCP (IEC 60870-5-104) y 20000/TCP (DNP3). Estos puertos suelen quedar abiertos por defecto, permitiendo conexiones externas sin autenticación. Un atacante con conocimiento de estos servicios puede interactuar con los dispositivos, modificar parámetros o incluso desactivar sistemas críticos.

Otra vulnerabilidad relacionada con los puertos abiertos es la presencia de servicios administrativos innecesarios, como acceso remoto mediante SSH, Telnet o RDP, que muchas veces se configuran sin medidas de seguridad adecuadas. La falta de restricciones en estos servicios facilita ataques de fuerza bruta, robo de credenciales y ejecución de comandos no autorizados.

Falta de Segmentación de Red

Uno de los errores más comunes en las redes industriales es la ausencia de una segmentación de red adecuada, lo que permite que dispositivos críticos sean accesibles desde cualquier punto dentro de la infraestructura. En muchos casos, las redes de control están conectadas directamente a las redes corporativas de TI sin restricciones, lo que expone los sistemas industriales a ataques originados desde entornos empresariales.

La falta de segmentación facilita ataques de movimiento lateral, donde un atacante que compromete un dispositivo menos crítico puede desplazarse dentro de la red hasta alcanzar sistemas esenciales como PLCs o servidores SCADA. Además, en caso de un incidente de seguridad, la ausencia de barreras dificulta la contención del ataque, permitiendo que se propague rápidamente por toda la infraestructura.

Otro problema derivado de la falta de segmentación es la exposición innecesaria de dispositivos a usuarios no autorizados. En redes mal configuradas, cualquier empleado con acceso a la red podría comunicarse con sistemas de control, modificar configuraciones o ejecutar comandos sin restricciones. Esto aumenta el riesgo de errores operativos, accesos indebidos y sabotaje interno.

Para mitigar estos riesgos, se recomienda implementar una arquitectura basada en zonas y conduits, siguiendo el modelo de ISA/IEC 62443, donde se establezcan segmentos de red con distintos niveles de acceso y protecciones adecuadas. El uso de firewalls industriales, VLANs y reglas estrictas de control de tráfico ayuda a limitar la exposición de los sistemas más críticos.

Dispositivos Obsoletos

Muchas redes industriales dependen de equipos antiguos que no reciben actualizaciones de seguridad, lo que los convierte en un blanco fácil para atacantes. Dispositivos como PLCs, RTUs, sensores y servidores SCADA pueden estar operando con software desactualizado y sin soporte por parte del fabricante, dejando expuestas vulnerabilidades críticas.

La falta de actualizaciones no solo impide la corrección de fallos de seguridad, sino que también hace que estos dispositivos sean incompatibles con soluciones de ciberseguridad modernas. Muchos sistemas antiguos no soportan cifrado, autenticación fuerte o protocolos seguros, lo que limita las opciones para protegerlos.

Otro problema de los dispositivos obsoletos es la dificultad para reemplazarlos o actualizarlos, debido a su alto costo y la necesidad de mantener la compatibilidad con otros sistemas en la planta. Esto lleva a muchas empresas a postergar la modernización de su infraestructura, aumentando el riesgo de incidentes de seguridad.

Para reducir esta vulnerabilidad, es importante aplicar estrategias como la virtualización de sistemas antiguos, el uso de firewalls para aislar dispositivos obsoletos y la implementación de compensaciones de seguridad como monitoreo continuo y segmentación de red.

Falta de Monitoreo Continuo

El monitoreo continuo es fundamental para detectar actividades sospechosas y responder rápidamente a posibles incidentes de seguridad en las redes de control industrial. Sin embargo, muchas empresas no cuentan con herramientas especializadas para analizar el tráfico de red en sus sistemas industriales, lo que dificulta la identificación de ataques en tiempo real.

La falta de monitoreo permite que un atacante pueda infiltrarse en la red y operar durante largos períodos sin ser detectado. Ataques como el reconocimiento pasivo, la manipulación de comandos o la exfiltración de datos pueden pasar desapercibidos si no se cuenta con un sistema de detección de intrusiones (IDS) especializado para entornos industriales.

Otra consecuencia de la ausencia de monitoreo es la falta de visibilidad sobre el estado de los dispositivos. Muchos equipos industriales generan registros de eventos, pero si estos no son analizados, se pierden oportunidades de detectar anomalías antes de que se conviertan en problemas graves.

Exposición a Internet

Exponer sistemas industriales a internet sin las medidas de seguridad adecuadas es una de las vulnerabilidades más graves en las redes de control. Muchos dispositivos de control están

conectados directamente a la web para facilitar el acceso remoto, pero sin configuraciones seguras, lo que los deja vulnerables a ataques automatizados y escaneos maliciosos.

Herramientas como Shodan permiten a los atacantes identificar dispositivos industriales expuestos con facilidad, lo que ha llevado al aumento de ataques dirigidos a PLCs, HMI y sistemas SCADA conectados a internet. Sin una configuración adecuada, los atacantes pueden obtener acceso y manipular procesos críticos sin necesidad de explotar vulnerabilidades complejas.

Para mitigar este riesgo, es fundamental evitar la exposición directa de dispositivos industriales a internet y utilizar VPNs, firewalls y autenticación multifactor (MFA) para accesos remotos. Además, es recomendable implementar listas de control de acceso (ACL) y restringir conexiones solo a direcciones IP confiables.

Tabla 4

Resumen de las Vulnerabilidades en las ICN

Vulnerabilidad	Descripción
Protocolos inseguros	Uso de protocolos como Modbus, DNP3 y Profibus sin cifrado ni autenticación.
Puertos y servicios expuestos	Configuración con puertos abiertos sin restricciones de acceso.
Falta de segmentación de red	Conexión directa entre redes IT y OT sin restricciones.
Dispositivos obsoletos	Equipos sin actualizaciones ni soporte del fabricante.
Falta de monitoreo continuo	Ausencia de herramientas para la detección de anomalías en la red industrial.
Exposición a internet	Conexión de dispositivos industriales a la red sin seguridad adecuada.

Nota. En la tabla se realiza un resumen de vulnerabilidades en las ICN.

Evaluación de impacto de la explotación de vulnerabilidades en los sistemas de control industrial basado en casos de estudio.

La explotación de vulnerabilidades en ICS no solo representa un riesgo para la disponibilidad y confiabilidad de las operaciones, sino que también puede generar daños físicos, pérdidas económicas y afectaciones a la seguridad pública. Para comprender mejor estos riesgos, es importante evaluar el impacto real de ataques dirigidos a estos sistemas a partir de casos documentados.

A continuación, se analizarán cinco casos reales de ataques dirigidos a sistemas de control industrial (ICS), con el propósito de identificar las vulnerabilidades explotadas, los métodos utilizados por los atacantes y el impacto tangible que estos incidentes generaron en las infraestructuras afectadas. Este análisis permitirá comprender cómo las debilidades en la seguridad de estos sistemas pueden comprometer la disponibilidad, integridad y confiabilidad de los procesos industriales, afectando no solo a las organizaciones involucradas, sino también a sectores estratégicos y a la seguridad pública.

Para evaluar el impacto de la explotación de vulnerabilidades en los SCI, se seleccionaron los siguientes casos debido a su relevancia en la seguridad de infraestructuras críticas, la diversidad de sus técnicas de ataque y las consecuencias generadas a nivel operacional, económico, político y social.

- Stuxnet (2010) – Ataque a la planta nuclear de Irán
- BlackEnergy (2015) – Apagón en Ucrania
- Triton/Trisis (2017) – Ataque a sistemas de seguridad en plantas petroquímicas
- Colonial Pipeline (2021) – Ransomware DarkSide
- Ataques a la industria del agua en EE.UU. (2021)

Cada uno de estos casos proporciona una perspectiva única sobre la explotación de vulnerabilidades en SCI, permitiendo un análisis integral de los riesgos, impactos y estrategias de mitigación necesarias para proteger infraestructuras críticas.

Stuxnet (2010) - Ataque a la planta nuclear de Irán

El ataque de Stuxnet en 2010 marcó un hito en la historia de la ciberseguridad industrial, siendo considerado el primer ciberataque dirigido específicamente a un sistema de control industrial. Este malware altamente sofisticado fue diseñado para sabotear el programa nuclear de Irán, afectando directamente las centrifugadoras utilizadas en el enriquecimiento de uranio en la planta de Natanz. A diferencia de otros virus informáticos que buscan robar información o dañar sistemas indiscriminadamente, Stuxnet tenía un objetivo claro: alterar el funcionamiento de los controladores lógicos programables (PLC) de Siemens utilizados en la planta, sin ser detectado por los operadores (Falliere et al., 2011).

El ataque utilizó múltiples vulnerabilidades de día cero en sistemas Windows para propagarse y una vez dentro de la red, se dirigió específicamente a los PLC controladores de las centrifugadoras. Stuxnet modificó la velocidad de giro de las centrifugadoras, alternando entre aceleraciones y desaceleraciones extremas, lo que generó fallos mecánicos y redujo la eficiencia del programa nuclear iraní. Lo más preocupante de este ataque fue su capacidad de operar de manera encubierta, ya que manipulaba las señales enviadas a los sistemas de monitoreo para que los operadores no detectaran las alteraciones, permitiendo que el sabotaje ocurriera sin levantar sospechas inmediatas.

El impacto del ataque fue significativo, con estimaciones que indican que alrededor de 1,000 de las 5,000 centrifugadoras en la planta de Natanz fueron destruidas o gravemente dañadas. La sofisticación del malware y la selección precisa de su objetivo apuntan a la

participación de actores estatales en su desarrollo, con sospechas de que Estados Unidos e Israel estuvieron detrás de su creación. Este incidente puso en evidencia la vulnerabilidad de infraestructuras críticas ante ataques cibernéticos dirigidos y abrió la puerta a una nueva era en la guerra cibernética.

Explotación de vulnerabilidades

Vulnerabilidades de día Cero en Windows: Stuxnet aprovechó al menos cuatro vulnerabilidades de día cero en el sistema operativo Windows, lo que le permitió propagarse sin ser detectado. Estas vulnerabilidades incluían la ejecución remota de código y la elevación de privilegios, facilitando la infección de sistemas sin necesidad de interacción del usuario.

Explotación de Dispositivos USB para Propagación: el malware se propagaba a través de unidades USB infectadas, explotando una vulnerabilidad en la ejecución automática de archivos en Windows. Dado que la red de la planta de Natanz no estaba conectada a internet, este método permitió la infiltración del malware en los sistemas críticos cuando los empleados conectaban dispositivos USB contaminados.

Compromiso de Software SCADA de Siemens. Stuxnet estaba diseñado específicamente para atacar los controladores lógicos programables (PLC) de Siemens, utilizados en los sistemas de control industrial de la planta. Manipuló el software Step7 para modificar las instrucciones enviadas a los PLC sin que los operadores detectaran anomalías en el sistema de monitoreo.

Firma Digital Falsa para Evadir Detección. el malware utilizó certificados digitales robados de empresas legítimas (Realtek y JMicron) para aparentar ser software confiable. Esto le permitió evadir mecanismos de seguridad como el control de firmas digitales en Windows, retrasando su detección.

Modificación Encubierta de los Procesos Industriales. Stuxnet alteraba los parámetros de funcionamiento de las centrifugadoras de uranio, modificando la velocidad de rotación de manera intermitente. Mientras tanto, enviaba datos falsificados a los sistemas de monitoreo, haciendo que los operadores no percibieran el daño progresivo a los equipos hasta que fue demasiado tarde.

Identificadores CVE (Common Vulnerabilities and Exposures)

CVE-2010-2568: vulnerabilidad en el manejo de accesos directos (.LNK) en Windows que permitía la ejecución automática de código malicioso cuando se visualizaba un archivo de acceso directo en una unidad extraíble (USB). Permitió la propagación de Stuxnet en sistemas aislados mediante dispositivos USB infectados.

CVE-2010-2729: vulnerabilidad en el servicio de colas de impresión de Windows que permitía la ejecución remota de código. Facilitó la escalada de privilegios y la propagación del malware dentro de la red de la planta nuclear.

CVE-2010-2743: vulnerabilidad en el sistema de programación de tareas de Windows que permitía la escalada de privilegios. Stuxnet la utilizó para ejecutar código malicioso con privilegios administrativos en los sistemas infectados.

CVE-2010-2772: vulnerabilidad en el software Siemens WinCC y PCS7 (utilizados para la gestión de PLCs). Permitió el acceso no autorizado a los sistemas SCADA de Siemens, facilitando la manipulación de los procesos industriales.

Tabla 5

Impacto del Ataque a la Planta Nuclear de Irán

Categoría de Impacto	Descripción del Impacto
Impacto en la Operación Industrial	Sabotaje en las centrifugadoras de enriquecimiento de uranio, provocando su falla prematura y afectando el proceso de producción nuclear.
Impacto Económico y Financiero	Costos elevados para la reposición de las centrifugadoras dañadas y la implementación de medidas de seguridad adicionales.
Impacto en Infraestructura Crítica	Compromiso del sistema de control SCADA de Siemens, afectando la confiabilidad de la automatización industrial en la planta.
Impacto en la Seguridad Nacional	Retraso en el programa nuclear iraní, con implicaciones estratégicas y geopolíticas en el contexto de la seguridad internacional.
Impacto en la Confianza y Reputación	Impacto en la credibilidad de la seguridad cibernética de infraestructuras críticas, exponiendo vulnerabilidades en sistemas industriales.
Impacto en la Ciberseguridad Global	Demostración de la capacidad de los ciberataques dirigidos a infraestructuras críticas, elevando la preocupación en la comunidad internacional.

Nota. En la tabla se realiza un resumen del impacto del ataque a la planta nuclear de Irán.

La tabla muestra los impactos causados por el ataque Stuxnet en la planta nuclear de Irán en 2010. Este ataque afectó múltiples aspectos, desde la operatividad y la infraestructura hasta la seguridad nacional y la confianza en la ciberseguridad industrial. La manipulación del sistema de control SCADA de Siemens permitió el sabotaje de centrifugadoras de enriquecimiento de uranio, generando pérdidas económicas y retrasos en el programa nuclear iraní. Además, el ataque expuso vulnerabilidades en infraestructuras críticas, alertando a la comunidad internacional sobre los riesgos de ciberataques avanzados en sistemas industriales.

Tiempo de Recuperación

Varios meses (estimado). La reposición de centrifugadoras dañadas y la limpieza del malware requirieron un proceso prolongado debido a la complejidad del ataque y la naturaleza crítica de la infraestructura.

Costo de Inactividad

- Alto (no cuantificado públicamente, pero significativo). Incluyó:
- Reemplazo de equipos físicos (1,000 centrifugadoras afectadas).
- Retrasos en el programa nuclear iraní (impacto estratégico).
- Costos de investigación y medidas de seguridad posteriores.

Severidad del Incidente (Crítico)

- Primer ataque cibernético con daños físicos verificables en infraestructura crítica.
- Implicaciones geopolíticas y de seguridad nacional.

BlackEnergy (2015) - Apagón en Ucrania

El ataque de BlackEnergy en 2015 dirigido contra la red eléctrica de Ucrania, dejó sin servicio a aproximadamente 230,000 personas en pleno invierno, lo que generó un impacto significativo en la estabilidad del país. BlackEnergy, un malware originalmente diseñado para espionaje y sabotaje, evolucionó hasta convertirse en una herramienta de ataque dirigida específicamente contra sistemas de control industrial, lo que permitió a los atacantes comprometer las estaciones de distribución de energía (Cherepanov & Lipovsky, 2017).

El ataque se llevó a cabo en varias etapas. En primer lugar, los ciberdelincuentes utilizaron correos electrónicos de phishing con documentos infectados para obtener acceso inicial a los sistemas de las compañías eléctricas. Una vez dentro, los atacantes utilizaron credenciales robadas para acceder a los sistemas SCADA, tomando el control de los interruptores de energía y desconectando varias subestaciones de la red. Además, implementaron un componente de borrado de disco (KillDisk) que eliminó archivos críticos y dejó los sistemas inutilizables, lo que dificultó la recuperación del servicio.

El impacto del ataque fue severo, pero las empresas afectadas lograron restaurar el servicio en un tiempo relativamente corto gracias a la capacidad de operar manualmente los sistemas de energía. Sin embargo, el incidente dejó en evidencia las vulnerabilidades de las infraestructuras críticas frente a amenazas cibernéticas avanzadas. BlackEnergy no solo interrumpió el suministro eléctrico, sino que también afectó sistemas de telecomunicaciones y dejó inutilizables dispositivos clave para la supervisión y recuperación de la red, lo que amplificó el daño y complicó la respuesta ante el incidente(Cherepanov, 2017).

El ataque a la red eléctrica de Ucrania en 2015 es un claro ejemplo de la creciente militarización del ciberespacio y del riesgo que enfrentan las infraestructuras críticas en todo el mundo. La sofisticación de la operación y la selección estratégica del objetivo apuntan a la posible participación de actores estatales en el ataque.

Explotación de Vulnerabilidades

Phishing y Credenciales Comprometidas: los atacantes utilizaron correos electrónicos de phishing con documentos maliciosos que contenían macros de Microsoft Office para infectar los sistemas con malware BlackEnergy3. Una vez que los empleados ejecutaban los archivos adjuntos, los atacantes obtenían acceso inicial a la red de TI.

Uso de Puertas Traseras (backdoors): los atacantes instalaron herramientas de acceso remoto (RATs) y shellcodes para moverse lateralmente dentro de la red y comprometer estaciones de trabajo y servidores críticos.

Desactivación de Sistemas de Supervisión y Respuesta: se explotaron vulnerabilidades en el software de administración de infraestructura SCADA para deshabilitar los sistemas de monitoreo de las subestaciones eléctricas.

Uso de KillDisk para sabotear recuperación. se implementó el malware KillDisk, que eliminó archivos clave en estaciones de trabajo y servidores, dificultando la restauración de los sistemas después del ataque. También se eliminaron los registros del sistema para evitar el análisis forense del ataque.

Ataque a Sistemas De Acceso Remoto. los atacantes explotaron configuraciones débiles en VPNs y sistemas de acceso remoto utilizados por los operadores de energía, permitiéndoles tomar el control manual de los interruptores eléctricos y desconectar el suministro eléctrico.

Identificadores CVE (Common Vulnerabilities and Exposures)

CVE-2014-4114: vulnerabilidad en OLE de Windows que permitía la ejecución de código arbitrario al abrir archivos maliciosos. Se utilizó en correos de phishing con documentos de PowerPoint maliciosos.

CVE-2015-2360: vulnerabilidad en Microsoft Office que permitía la ejecución de macros maliciosas. Facilitó la infección inicial en las redes eléctricas.

CVE-2012-0158: vulnerabilidad en Microsoft Word que permitía la ejecución de código arbitrario a través de archivos RTF maliciosos. Se utilizó en campañas de spear-phishing para comprometer equipos.

CVE-2015-2545: vulnerabilidad en el manejo de gráficos de Microsoft Office que permitía ejecución de código remoto. Usada para desplegar el malware en redes comprometidas.

CVE-2014-4113: escalada de privilegios en Windows que permitía a los atacantes obtener permisos de administrador. Permitió a los atacantes tomar control total de los sistemas infectados.

CVE-2015-8103: vulnerabilidad en el software de administración SCADA de Siemens WinCC que permitía ejecución remota de código. Se usó para comprometer sistemas de control industrial en la red eléctrica.

Tabla 6

Impacto del ataque BlackEnergy (2015) en Ucrania.

Categoría de Impacto	Descripción del Impacto
Impacto Energético	Apagón masivo afectó a más de 225,000 personas en Ucrania durante varias horas.
Impacto Infraestructura Crítica	Compromiso de sistemas SCADA y estaciones de distribución eléctrica, interrumpiendo el control de la red.
Impacto Económico	Pérdidas financieras por interrupción del suministro eléctrico y costos de recuperación de infraestructura afectada.
Impacto Operacional	Afectó la capacidad de respuesta de las compañías eléctricas debido a la sobreescritura de firmware en equipos clave.
Impacto Ciberseguridad	Demostró la vulnerabilidad de las infraestructuras críticas a ataques avanzados de malware y APTs.
Impacto Político y Geopolítico	Incrementó tensiones entre Ucrania y Rusia, con acusaciones de ciberataques como parte de una estrategia de guerra híbrida.
Impacto Social	Impacto en la vida cotidiana de la población debido a la falta de electricidad en invierno, afectando hospitales, transporte y comunicaciones.

Nota. En la tabla se realiza un resumen del impacto del ataque de BlackEnergy.

La tabla muestra los principales impactos del ataque BlackEnergy (2015) en Ucrania, evidenciando cómo un ciberataque puede afectar no solo la infraestructura tecnológica sino también el ámbito social, económico y político. Se destaca la afectación en la red eléctrica, la interrupción de servicios esenciales y el costo económico derivado de la recuperación del sistema. Además, el ataque marcó un precedente en el uso de ciberarmas contra infraestructuras críticas, generando preocupaciones a nivel global sobre la seguridad de los sistemas SCADA y de distribución eléctrica.

Tiempo de Recuperación

6 horas a 1 día (restauración parcial). Aunque el apagón duró horas, la recuperación completa de sistemas IT/OT afectados tomó semanas debido al componente KillDisk.

Costo de inactividad

- Millones de dólares (impacto regional).
- Pérdidas por interrupción en comercio, transporte y servicios esenciales.
- Costos de reparación de sistemas SCADA y equipos dañados.

Severidad del incidente (Alto)

- Primer apagón eléctrico causado por un ciberataque.
- Demostró la vulnerabilidad de redes eléctricas ante ataques coordinados.

Triton/Trisis (2017) - Ataque a sistemas de seguridad en plantas petroquímicas

El ataque Triton, también conocido como Trisis, ocurrido en 2017, fue diseñado específicamente para comprometer los sistemas de seguridad de una planta petroquímica. Este malware fue descubierto en una instalación en Medio Oriente cuando los atacantes intentaron modificar el sistema de seguridad industrial Triconex, fabricado por Schneider Electric. Los sistemas Triconex son críticos en la industria, ya que están diseñados para detectar condiciones peligrosas y en caso de emergencia, apagar automáticamente los procesos para prevenir daños a la infraestructura, pérdidas económicas y riesgos a la vida humana (Pinto et al., 2018).

Los ciberdelincuentes lograron acceso a la red de la planta a través de una conexión remota y tras un largo período de reconocimiento, implantaron el malware en los controladores de seguridad Triconex. Su objetivo era reprogramar estos dispositivos para deshabilitar los mecanismos de protección y permitir potencialmente un ataque destructivo. Sin embargo, debido a un error en la implementación del código malicioso, se activó un fallo en el sistema de

seguridad que detuvo los procesos industriales, lo que llevó a la detección del ataque antes de que los atacantes pudieran causar un daño significativo.

El impacto del ataque Triton fue alarmante porque representó un intento directo de sabotaje a una infraestructura crítica con potencial para causar explosiones, incendios o derrames químicos. A diferencia de ataques anteriores que buscaban espionaje o interrupción de operaciones, Triton tenía como objetivo comprometer la seguridad física de la planta y de sus trabajadores. Este ataque demostró la vulnerabilidad de los sistemas de seguridad industrial ante amenazas cibernéticas avanzadas y evidenció que los atacantes pueden utilizar estos sistemas, diseñados para proteger vidas, como armas para provocar accidentes catastróficos.

El incidente Triton subrayó la importancia de la segmentación de redes, la implementación de mecanismos de detección de anomalías y el fortalecimiento de la seguridad en sistemas de control industrial. La sofisticación del ataque y la elección del objetivo sugieren la posible participación de actores estatales, lo que eleva la amenaza de ciberataques dirigidos a infraestructuras críticas en el futuro. Este evento sirvió como una advertencia para la industria petroquímica y otros sectores estratégicos, impulsando mejoras en la seguridad de los sistemas industriales y reforzando la cooperación entre gobiernos y empresas para mitigar riesgos de ciberseguridad en entornos industriales.

Explotación de Vulnerabilidades

Acceso no Autorizado a la Red OT. los atacantes lograron infiltrarse en la red de tecnología operativa de la planta petroquímica, probablemente a través de credenciales comprometidas o explotación de un sistema sin segmentación adecuada entre IT y OT.

Vulnerabilidades en el Software De Ingeniería de Triconex. se explotó una debilidad en el software de programación y gestión de controladores Triconex. Se sospecha que los

atacantes usaron herramientas de administración legítimas para desplegar código malicioso sin ser detectados.

Falta de Protección en la Autenticación del Firmware de Triconex: el malware Triton modificó la lógica de los controladores de seguridad, lo que sugiere que la autenticación del firmware no era suficientemente robusta o que los atacantes encontraron un método para evadirla.

Habilitación del "Modo de Programación" en Triconex: los atacantes pusieron los controladores en un estado de modo de programación, lo que les permitió modificar su comportamiento. Esta acción requiere acceso privilegiado, lo que indica que lograron escalar privilegios en el sistema.

Ausencia de Monitoreo Y Detección De Actividad Anómala. no se detectó de inmediato la manipulación de los controladores de seguridad, lo que sugiere la falta de monitoreo en tiempo real o mecanismos de alerta temprana en la red industrial.

Tabla 7

Impacto del Ataque Triton/Trisis

Categoría de impacto	Descripción
Compromiso de los Sistemas de Seguridad (SIS)	El malware Triton modificó la lógica de los controladores Triconex, lo que pudo haber deshabilitado medidas de seguridad críticas.
Riesgo de accidentes catastróficos	Al afectar los SIS, el ataque pudo haber provocado explosiones, incendios o derrames de sustancias peligrosas.
Interrupción operativa	La detección del ataque llevó al apagado de la planta para evitar consecuencias mayores, generando pérdidas económicas y retrasos en la producción.
Impacto financiero	Se estima que la empresa afectada incurrió en costos elevados por investigaciones, recuperación de sistemas y medidas de seguridad adicionales.
Evolución de las amenazas a sistemas industriales	Triton demostró la vulnerabilidad de los sistemas de seguridad en entornos industriales, incentivando a otros actores maliciosos a desarrollar ataques similares.

Reputación y confianza afectada	El ataque evidenció fallos en la ciberseguridad de infraestructuras críticas, afectando la confianza en los protocolos de seguridad de la industria.

Nota. En la tabla se realiza un resumen del impacto del ataque de Triton.

Esta tabla resume los principales impactos que causó el ataque Triton/Trisis en la industria petroquímica. Uno de los efectos más críticos fue el compromiso de los Sistemas Instrumentados de Seguridad (SIS), cuya función es proteger la integridad de los procesos industriales. El ataque también puso en riesgo la seguridad física de las instalaciones y el personal, ya que la manipulación de estos sistemas pudo haber resultado en explosiones o accidentes graves.

Tiempo de Recuperación

Semanas a meses. La planta detuvo operaciones para investigar y reemplazar los controladores Triconex comprometidos.

Costo de Inactividad

- Alto (no revelado públicamente, pero estimado en decenas de millones).
- Parálisis de producción.
- Reemplazo de hardware y software de seguridad.

Severidad del INCIDENte (Crítico)

- Primer ataque dirigido a Sistemas Instrumentados de Seguridad (SIS), con potencial para causar catástrofes industriales (explosiones, fugas químicas).

Colonial Pipeline (2021) - Ransomware DarkSide

El ataque a Colonial Pipeline en mayo de 2021 representó uno de los incidentes de ciberseguridad más graves en la historia de Estados Unidos, evidenciando la vulnerabilidad de la infraestructura crítica ante amenazas como el ransomware. Colonial Pipeline es una de las

principales redes de oleoductos del país, transportando aproximadamente el 45% del combustible consumido en la costa este. El ataque fue perpetrado por el grupo de ciberdelincuentes DarkSide, quienes utilizaron ransomware para cifrar los sistemas de la empresa y exigir un rescate en criptomonedas a cambio de la restauración del acceso. Como consecuencia, la empresa tuvo que suspender sus operaciones durante varios días, generando una crisis en el suministro de combustible que afectó a millones de personas (Agency, 2021).

El ataque comenzó cuando los ciberdelincuentes lograron infiltrarse en la red de Colonial Pipeline a través de credenciales comprometidas en una VPN sin autenticación multifactor. Una vez dentro, desplegaron el ransomware, que cifró los archivos críticos de la empresa, impidiendo el acceso a los sistemas administrativos y operativos. Aunque el malware no afectó directamente a los sistemas de control industrial (ICS), la empresa tomó la decisión de cerrar temporalmente el oleoducto como medida de precaución, lo que provocó escasez de combustible, aumentos en los precios y compras de pánico en varias regiones de Estados Unidos.

El impacto del ataque no solo se reflejó en la interrupción del servicio, sino también en las decisiones tomadas por la empresa. Colonial Pipeline pagó un rescate de 4.4 millones de dólares en Bitcoin para recuperar el acceso a sus sistemas, aunque posteriormente, el gobierno de Estados Unidos logró recuperar parte de los fondos. Este incidente puso en evidencia la creciente amenaza del ransomware en infraestructuras críticas y la dificultad que enfrentan las empresas para defenderse de ataques cada vez más sofisticados. Además, expuso la necesidad de mejorar la ciberseguridad en sectores estratégicos para evitar que actores malintencionados puedan paralizar servicios esenciales (Gawazah, 2024).

A raíz del ataque, el gobierno estadounidense tomó medidas para reforzar la seguridad en infraestructuras críticas, implementando regulaciones más estrictas y fomentando la colaboración

entre el sector privado y las agencias de seguridad. También se intensificaron las estrategias para combatir el ransomware, incluyendo la persecución de grupos cibercriminales y la promoción de buenas prácticas de ciberseguridad, como la segmentación de redes, la implementación de autenticación multifactor y la realización de auditorías de seguridad constantes.

El ataque a Colonial Pipeline demostró el alto impacto que pueden tener las amenazas cibernéticas en la vida cotidiana y subrayó la urgencia de adoptar medidas proactivas para fortalecer la resiliencia de infraestructuras críticas ante futuros ataques.

Explotación de Vulnerabilidades

Credenciales Comprometidas en un Acceso Remoto VPN sin Autenticación Multifactor (MFA). los atacantes obtuvieron credenciales de acceso a una red privada virtual (VPN) utilizada por Colonial Pipeline. Se presume que las credenciales fueron filtradas en la dark web debido a una brecha de seguridad previa en otra plataforma utilizada por un empleado.

Como la VPN no tenía habilitada la autenticación multifactor (MFA), los atacantes pudieron acceder sin necesidad de validaciones adicionales.

Falta de Segmentación en la Infraestructura de Red. la red operativa (OT) y la red de tecnología de la información (IT) no estaban completamente aisladas, lo que permitió que el ataque dirigido a sistemas IT afectara indirectamente las operaciones de la empresa.

Como medida de contención, Colonial Pipeline apagó preventivamente sus sistemas para evitar la propagación del ransomware a los sistemas industriales.

Uso de Técnicas de Movimiento Lateral y Ejecución de Ransomware. Una vez dentro de la red, los atacantes usaron herramientas comunes como Mimikatz y PsExec para moverse dentro del entorno y escalar privilegios.

Posteriormente, desplegaron el ransomware DarkSide, cifrando archivos críticos y exigiendo un rescate de 4,4 millones de dólares en Bitcoin.

Falta de Monitoreo Avanzado De Amenazas. Aunque Colonial Pipeline tenía medidas de seguridad en su infraestructura, el ataque no fue detectado en su etapa inicial, lo que permitió a los atacantes operar sin ser identificados hasta que el ransomware fue ejecutado.

Identificadores CVE (Common Vulnerabilities and Exposures)

CVE-2020-3259. vulnerabilidad en dispositivos Cisco que permite a atacantes remotos acceder a información sensible a través de solicitudes específicas.

CVE-2023-20269. Vulnerabilidad en el software de Cisco que podría permitir a un atacante remoto no autenticado realizar ataques de fuerza bruta o establecer sesiones VPN SSL sin cliente utilizando credenciales válidas.

CVE-2024-5921. Vulnerabilidad en clientes VPN de Palo Alto Networks que podría permitir la ejecución remota de código en dispositivos de los usuarios.

CVE-2024-29014. Vulnerabilidad en clientes VPN de SonicWall que podría ser explotada para ejecutar código de forma remota en los dispositivos de los usuarios.

Tabla 8

Impacto del Ataque de Ransomware DarkSide

Categoría de impacto	Descripción
Interrupción de operaciones	Colonial Pipeline cerró sus operaciones para contener el ataque, afectando el transporte de combustible en EE.UU.
Pérdidas económicas	La empresa pagó un rescate de **$4.4 millones** en Bitcoin y enfrentó costos adicionales por la restauración del sistema.
Afectación a la infraestructura energética	Se generaron escasez y compras de pánico en gasolineras de la costa este de EE.UU.
Deterioro de la confianza y reputación	La confianza en la ciberseguridad de la empresa se vio afectada, causando preocupación en el sector energético.
Cambio en normativas y regulaciones	El ataque llevó al gobierno de EE.UU. a fortalecer regulaciones de ciberseguridad para infraestructuras críticas.
Fallos de seguridad en la red	Se identificó que los atacantes accedieron a la red a través de credenciales de VPN sin autenticación multifactor (MFA).

Impacto en la población y sociedad	El aumento en los precios del combustible y la escasez impactaron a millones de personas en EE.UU.

Nota. En la tabla se realiza un resumen del impacto del ataque de DarkSide.

La tabla resume los principales impactos del ataque de ransomware DarkSide a Colonial Pipeline en 2021. Este incidente afectó la operación del mayor oleoducto de EE.UU., causando interrupciones en el suministro de combustible, pérdidas económicas millonarias, daño reputacional y regulaciones más estrictas en ciberseguridad. Además, expuso vulnerabilidades tecnológicas, como el acceso no autorizado mediante credenciales comprometidas y generó un impacto social significativo debido a la escasez y el aumento de precios del combustible.

Tiempo de Recuperación

5 días (paralización total del oleoducto). La reactivación gradual tomó una semana adicional.

Costo de Inactividad

4.4 millones (rescate pagado) + 50 millones en pérdidas indirectas.

Escasez de combustible en la costa este de EE.UU.

Aumento de precios y compras de pánico.

Severidad del Incidente (Alto)

Mayor interrupción por ransomware en infraestructura crítica en EE.UU.

Impacto en cadenas de suministro y políticas de ciberseguridad gubernamentales.

Ataques a la Industria Del agua en EE.UU. (2021)

En 2021, se registraron múltiples intentos de ciberataques dirigidos a plantas de tratamiento de agua en Estados Unidos, lo que evidenció la vulnerabilidad de la infraestructura crítica ante amenazas cibernéticas. Uno de los casos más alarmantes ocurrió en la planta de

tratamiento de agua en Oldsmar, Florida donde un atacante logró acceder al sistema de control y modificó los niveles de hidróxido de sodio (soda cáustica) en el agua potable. Afortunadamente, un operador detectó la actividad sospechosa a tiempo y revirtió los cambios antes de que afectaran la seguridad del suministro de agua para miles de personas.

El ataque a la planta de Oldsmar se realizó a través de una conexión remota no segura en el software TeamViewer, lo que permitió al atacante manipular los sistemas de control industrial (ICS). Este incidente dejó en evidencia la falta de medidas de seguridad adecuadas en las instalaciones de agua, como la ausencia de autenticación multifactor y el uso de credenciales débiles.

Después de esto se identificaron otros intentos de ataque a plantas de agua en diferentes estados del país, algunos de ellos vinculados a grupos de ciberdelincuentes y actores patrocinados por estados extranjeros que buscaban comprometer la infraestructura crítica de EE.UU.

Estos ataques resaltaron la creciente amenaza cibernética en el sector del agua y la necesidad de mejorar la seguridad en sistemas de control industrial. Muchas plantas aún utilizan tecnologías obsoletas y carecen de segmentación adecuada en sus redes, lo que facilita el acceso a actores malintencionados. Además, la falta de capacitación en ciberseguridad para el personal operativo agrava el problema, ya que los ataques pueden explotar errores humanos o configuraciones inadecuadas en los sistemas de control.

Como respuesta a estos incidentes, el gobierno de EE. UU. tomó medidas para reforzar la seguridad de las infraestructuras críticas, incluyendo la emisión de directrices por parte de la Agencia de Ciberseguridad y Seguridad de Infraestructura (CISA) y el impulso de regulaciones más estrictas para la protección de plantas de agua y otros servicios esenciales. A pesar de estos

esfuerzos, los ataques a la industria del agua en 2021 demostraron la urgencia de fortalecer la ciberseguridad en este sector, ya que una intrusión exitosa podría tener consecuencias catastróficas para la salud pública y la seguridad nacional.

Explotación de Vulnerabilidades

Acceso Remoto Inseguro. se usaron herramientas de acceso remoto como TeamViewer, que estaban mal configuradas o protegidas con credenciales débiles o reutilizadas. Los atacantes lograron ingresar a los sistemas de control sin necesidad de autenticación multifactor (MFA).

Credenciales Comprometidas. las credenciales de acceso eran compartidas entre múltiples operadores, lo que facilitó el acceso no autorizado. No se aplicaron políticas estrictas de gestión de contraseñas.

Falta de Segmentación De Redes. la red de tecnología operativa (OT) estaba conectada directamente a la red de TI, sin una segmentación adecuada, permitiendo que un atacante en la red corporativa accediera a los sistemas de control.

Sistemas Obsoletos Y Sin Parches. los sistemas SCADA y HMI (interfaces de control) utilizaban versiones antiguas de software con vulnerabilidades conocidas.

Identificadores CVE (Common Vulnerabilities and Exposures)

CVE-2021-34858. vulnerabilidad en TeamViewer que permite a atacantes remotos ejecutar código arbitrario mediante la manipulación de archivos TVS.

CVE-2021-35005. vulnerabilidad en TeamViewer que permite a atacantes locales divulgar información sensible debido a una validación inadecuada de datos suministrados por el usuario.

- **CVE-2019-13943.** vulnerabilidad en módulos Ethernet EN100 que afecta a variantes DNP3, IEC 61850, IEC104, Modbus TCP y PROFINET IO, permitiendo posibles ataques de denegación de servicio.
- **CVE-2021-22772.** Vulnerabilidad en Schneider Electric Easergy T200 que permite operaciones no autorizadas al omitir la autenticación en las variantes Modbus, IEC104 y DNP3.

Tabla 9

Impactos Causados por El Ataque a la Industria del Agua en EE.UU

Categoría de Impacto	Descripción del Impacto
Interrupción del servicio	Los atacantes intentaron modificar los niveles de productos químicos en el agua potable, lo que pudo haber afectado el suministro de agua segura.
Riesgo para la salud pública	La alteración de los niveles de hidróxido de sodio (lejía) pudo haber generado intoxicaciones masivas si no se detectaba a tiempo.
Vulnerabilidad en infraestructuras críticas	Se evidenció la falta de seguridad en los sistemas SCADA y de control industrial, exponiendo la infraestructura del agua a posibles ataques futuros.
Impacto económico	Se requirió una inversión adicional en seguridad y modernización de los sistemas, además de posibles costos legales y compensaciones.
Confianza pública afectada	La población perdió confianza en la seguridad del suministro de agua, lo que llevó a una mayor preocupación sobre la ciberseguridad en infraestructuras críticas.

Nota. En la tabla se realiza un resumen del impacto del ataque a la industria del Agua.
Esta tabla muestra los principales impactos causados por el ataque a la industria del agua en EE.UU. en 2021. Se destaca cómo la vulnerabilidad de los sistemas permitió un intento de manipulación química del agua potable, lo que pudo haber tenido graves consecuencias para la salud pública. Además, se evidencian los costos económicos y el daño a la confianza de los ciudadanos en la seguridad de estos sistemas.

Tiempo de Recuperación

Horas (en Oldsmar, Florida, gracias a la detección temprana). Otras plantas requirieron días para asegurar sistemas.

Costo de Inactividad

- Variable (desde miles hasta millones en modernización de seguridad).
- Costos de auditorías y actualización de sistemas SCADA.
- Multas por incumplimiento de regulaciones

Severidad del incidente (*Moderado a Alto)*

- Riesgo de intoxicación masiva (evitado por intervención humana).
- Exposición de vulnerabilidades en infraestructura hídrica.

El análisis de los casos de estudio ha permitido evidenciar cómo las vulnerabilidades presentes en los sistemas de control industrial (ICS) pueden ser explotadas por actores maliciosos con diferentes niveles de sofisticación, generando consecuencias operacionales, económicas y de seguridad física.

A lo largo de los últimos años, incidentes como Stuxnet, Industroyer, Triron y ataques más recientes como el que afectó la planta de agua en Oldsmar, Florida, han dejado en claro que los entornos OT ya no están aislados ni protegidos por defecto y que sus debilidades pueden ser usadas como vectores de ataque para comprometer infraestructuras críticas.

En estos casos, se han observado patrones comunes como el uso de protocolos industriales inseguros, acceso remoto sin controles adecuados, ausencia de segmentación de red, software sin parches de seguridad y fallos en la autenticación o autorización de usuarios. Además, muchos de estos sistemas operaban con tecnología obsoleta, sin mecanismos de monitoreo activo que permitieran detectar o responder a los ataques en tiempo real.

Este panorama evidencia que las vulnerabilidades en los niveles de control y supervisión de la pirámide CIM no son hipotéticas, sino que han sido explotadas exitosamente en entornos reales, con impacto directo sobre procesos físicos, como apagones masivos, sabotaje de procesos químicos o alteraciones en sistemas de seguridad industrial.

Propuesta de Estrategias de Mitigación para ICS

Los sistemas de control industrial (ICS) representan el corazón operativo de infraestructuras críticas en sectores como la energía, manufactura, transporte y aguas. La creciente interconexión entre redes de tecnología de la información (TI) y de tecnología operacional (OT) ha ampliado la superficie de ataque de estos entornos, generando la necesidad de estrategias proactivas de mitigación que garanticen su seguridad y disponibilidad continua (Dragos, 2025).

En este contexto, se propone una serie de estrategias de mitigación enfocadas en tres pilares fundamentales: segmentación de redes, gestión de parches y controles de acceso físico. Estas acciones forman parte de un enfoque de defensa en profundidad que permite reducir la exposición a amenazas y mejorar la resiliencia operativa de los ICS.

Segmentación de Redes como Primera Línea De Defensa

La segmentación de redes es una de las estrategias más efectivas y recomendadas para contener incidentes de ciberseguridad en entornos industriales. Su objetivo principal es limitar el movimiento lateral de un atacante dentro de la red, estableciendo barreras entre zonas críticas y zonas menos sensibles. En los sistemas de control industrial, esta medida es importante debido a la criticidad y la baja tolerancia al fallo que caracteriza a estos entornos(Djebbar & Nordstrom, 2023).

En el contexto de los ICS, existen dos formas principales de segmentación: segmentación lógica y segmentación física. La segmentación lógica se implementa a través de tecnologías como VLANs, firewalls, reglas de acceso o listas de control (ACLs), mientras que la segmentación física implica el aislamiento de componentes a través de conexiones independientes o redes separadas.

Una de las metodologías más completas y reconocidas para aplicar segmentación en entornos industriales es el modelo de zonas y conductos de la norma IEC 62443. En este modelo, se define una zona como un grupo de activos con requisitos comunes de ciberseguridad y un conducto como el canal seguro a través del cual fluye la comunicación entre zonas. Esta arquitectura permite aplicar controles diferenciados y específicos según la criticidad del proceso, favoreciendo una implementación escalonada y flexible (Wang et al., 2023).

El Instituto Nacional de Estándares y Tecnología (NIST), a través del documento NIST SP 800-82, también recomienda aplicar segmentación entre las redes IT y OT, utilizando mecanismos como firewalls industriales con políticas específicas para ICS y zonas desmilitarizadas (DMZ) para facilitar la comunicación entre servidores de aplicación, SCADA, HMI y estaciones de ingeniería.

Uno de los beneficios más relevantes de la segmentación es su capacidad para contener incidentes de seguridad. Por ejemplo, en el ataque Triton (2017) el grupo de atacantes logró acceder al sistema de seguridad de la planta petroquímica debido a una segmentación deficiente que permitió el acceso desde redes corporativas hacia el entorno OT. Este incidente evidenció cómo la falta de fronteras claras puede exponer procesos industriales a sabotajes con consecuencias físicas.

Entre las buenas prácticas para una segmentación efectiva en ICS se destacan:

- Separar completamente las redes IT de las redes OT, evitando rutas directas o túneles VPN sin inspección.
- Implementar firewalls con inspección profunda de paquetes (DPI) entre zonas, capaces de entender protocolos industriales como Modbus, DNP3 o OPC UA.

- Limitar el tráfico entre zonas únicamente a lo necesario, aplicando el principio de mínimo privilegio en las comunicaciones.
- Desplegar sensores de monitoreo (IDS/IPS) en puntos estratégicos para detectar tráfico no autorizado entre zonas.

La segmentación no debe considerarse una medida única, sino como parte de una arquitectura de defensa en profundidad, en la que cada zona segmentada también incluye controles específicos según su nivel de exposición y criticidad. Su correcta implementación permite no solo mejorar la visibilidad y el control del entorno, sino también fortalecer la capacidad de respuesta ante incidentes.

Gestión de Parches y Actualizaciones Seguras

La gestión de parches y actualizaciones en los sistemas de control industrial representa un desafío técnico y organizacional considerable. A diferencia de los entornos tradicionales de TI, donde la aplicación de parches puede automatizarse o programarse sin mayores consecuencias, los ICS operan bajo condiciones estrictas de alta disponibilidad, donde cualquier interrupción puede traducirse en pérdidas económicas o riesgos para la seguridad física.

Además, muchos dispositivos industriales como PLC, RTU o HMI operan con firmware personalizado, sistemas operativos embebidos o aplicaciones desarrolladas en tecnologías obsoletas sin soporte activo, lo que limita las posibilidades de actualización o parches de seguridad. Esta situación genera una brecha temporal de exposición, en la cual los dispositivos son susceptibles a vulnerabilidades conocidas, pero aún no mitigadas.

Para enfrentar este problema, es importante establecer un proceso estructurado de gestión de parches, que contemple las siguientes etapas clave:

- Identificación De Activos Críticos: Mediante Inventarios Actualizados Y Sistemas De Gestión De Configuración (CMDB), Clasificando Los Activos Por Criticidad.
- Monitoreo Continuo De Vulnerabilidades: Utilizando Plataformas Como NIST NVD, CISA ICS Advisories, CVE Details O Los Boletines De Los Fabricantes (Ej. Siemens, Rockwell, Schneider).
- Evaluación De Riesgos: Antes De Aplicar Un Parche, Debe Analizarse Su Impacto En La Operación Y Su Urgencia O La Exposición Al Entorno.
- Pruebas En Entornos De Preproducción: Reproducir La Arquitectura En Laboratorios Controlados Para Validar La Compatibilidad Del Parche.
- Aplicación Segura: Programar Ventanas De Mantenimiento, Aplicar Parches En Fases O Con Técnicas De Blue-Green Deployment Cuando Sea Posible, Que Consiste En Tener Dos Entornos Casi Idénticos: Uno Activo (Blue) Que Está En Uso Por Los Usuarios Y Otro En Espera (Green) Donde Se Implementa La Nueva Versión Del Sistema O Parche.
- Verificación Posterior: Monitorear El Comportamiento Del Sistema Tras La Actualización Y Realizar Una Reversión (Rollback) Si Es Necesario.

En Ocasiones, Debido A Limitaciones Del Fabricante O A La Criticidad Del Proceso, No Es Posible Aplicar Parches. En Estos Casos Se Deben Implementar Controles Compensatorios, Como:

- Segmentación De Red Estricta Para Aislar El Activo Vulnerable.
- Monitoreo De Tráfico Con IDS Específicos Para Protocolos Industriales (Ej. Snort O Zeek Con Reglas Industriales).
- Reforzamiento Del Control De Accesos, Autenticación Multifactor Y Desactivación De Servicios Innecesarios.

Organizaciones Líderes Como ISA, NIST Y El European Union Agency For Cybersecurity (ENISA) Recomiendan Integrar La Gestión De Parches Dentro De Un Enfoque De Ciclo De Vida De Seguridad Industrial, Alineado Con Normativas Como IEC 62443-2-1 Y NIST CSF. Esto Garantiza Una Protección Continua, Documentada Y Adaptable A Las Necesidades Del Entorno Operativo(Firoozjaei Et Al., 2022)

Controles de Acceso Físico Y Lógico

En los sistemas de control industrial (ICS), los controles de acceso físico y lógico constituyen una capa importante de defensa frente a amenazas tanto internas como externas. A diferencia de entornos exclusivamente digitales, los ICS dependen de la protección tanto del hardware físico (como PLCs, tableros de control o estaciones HMI) como del acceso lógico a sistemas operativos, redes y software especializado. La ausencia de controles adecuados puede facilitar desde sabotajes físicos hasta intrusiones remotas no autorizadas.

Acceso Físico

El acceso físico no autorizado puede permitir manipulación directa de dispositivos de control, introducción de malware por medios físicos (por ejemplo, USB), o incluso sabotaje. Para mitigar estos riesgos, se recomiendan las siguientes medidas:

- Cerraduras electrónicas en gabinetes de control y cuartos de servidores.
- Sistemas de autenticación por tarjeta (RFID), huella digital o código PIN para personal autorizado.
- Monitoreo por sistemas de video vigilancia en áreas sensibles como salas SCADA, subestaciones o centros de datos industriales.
- Sensores de apertura y alarmas en puertas críticas.
- Registro de entradas y salidas a través de bitácoras físicas o sistemas digitales.

Estas medidas se pueden implementar en plantas industriales con zonas restringidas, donde la manipulación no autorizada de un solo componente puede tener consecuencias significativas

Acceso Lógico

El acceso lógico se refiere a la capacidad de un usuario o sistema para interactuar con dispositivos, software o redes a través de interfaces digitales. En ICS, es común encontrar dispositivos que carecen de autenticación fuerte, lo que incrementa su riesgo de explotación. Para contrarrestar esto, se deben aplicar:

- Autenticación multifactor (MFA): para todo acceso remoto o administrativo.
- Control de acceso basado en roles (RBAC): que limite privilegios de acuerdo con el perfil del usuario (operador, ingeniero, supervisor, auditor).
- Políticas de contraseñas robustas: longitud mínima, complejidad, expiración periódica y bloqueo por intentos fallidos.
- Registro y auditoría de accesos lógicos: mediante sistemas de logging centralizado o SIEM.
- Desactivación de interfaces y servicios no utilizados, incluyendo puertos USB, puertos de red o protocolos innecesarios.

Normativas y Estándares Aplicables

Varios marcos regulatorios destacan la importancia de estos controles. La norma IEC 62443-3-3 detalla requisitos para acceso físico seguro y control lógico. De igual forma el NIST SP 800-53 propone controles específicos como PE-2 (Control de acceso físico), AC-3 (Control de acceso lógico) y IA-2 (Identificación y autenticación del usuario). La ISO/IEC 27001 también incluye controles aplicables al contexto OT, especialmente en su Apéndice A.

Buenas Prácticas Complementarias

- Realizar evaluaciones periódicas de accesos, para identificar cuentas inactivas, privilegios excesivos o configuraciones erróneas.
- Aplicar el principio de mínimo privilegio para toda interacción con el sistema.
- Configurar tiempos de expiración de sesión en interfaces HMI o SCADA.
- Implementar soluciones de gestión de identidades (IAM) adaptadas al entorno industrial.

La implementación conjunta de controles físicos y lógicos no solo protege la infraestructura frente a accesos no autorizados, sino que también refuerza la cultura de seguridad en la organización.

Modelo de seguridad por Capas para ICS Basado en NIST SP 800-82 y IEC 62443-3-3

La ciberseguridad en sistemas de control industrial (ICS) no puede depender de una única capa de defensa. Dado que las amenazas pueden provenir de múltiples vectores internos, externos, físicos, lógicos o incluso humanos, se requiere un enfoque estructurado y coordinado. El modelo de seguridad por capas para ICS propone precisamente eso: una arquitectura de seguridad con múltiples capas, que se refuerzan mutuamente para proteger la operación frente a amenazas complejas y persistentes (Makrakis et al., 2021).

Este modelo tiene como principio que cada capa de defensa actúe como una barrera ante posibles fallos o compromisos de las demás, retardando o deteniendo el avance de un atacante. En el contexto de los ICS, El modelo debe adaptarse a las particularidades de los entornos OT, donde la seguridad no puede comprometer la disponibilidad ni la integridad de los procesos industriales.

Una arquitectura integrada para ICS puede estructurarse en las siguientes capas:

Capa Física

- Controles de acceso físico: puertas, cerraduras, vigilancia, RFID.
- Protección contra sabotajes o manipulaciones de hardware.
- Redundancia física (alimentación eléctrica, redes, etc.).

Capa de Red

- Segmentación de redes (VLAN, DMZ, firewalls).
- Monitoreo de tráfico (IDS/IPS industrial).
- Control de tráfico OT–IT y reglas específicas para protocolos industriales.

Capa de Sistema Operativo y Software

- Gestión de parches y actualizaciones.
- Hardening del sistema (desactivación de servicios no utilizados, configuraciones seguras).
- Control de integridad mediante listas blancas o validación de hashes.

Capa de Aplicación

- Autenticación de usuarios (MFA, RBAC).
- Auditoría de eventos y registro de logs.
- Gestión segura de interfaces HMI, SCADA y bases de datos.

Capa Organizacional

- Concienciación del personal y formación continua.
- Gestión de incidentes, procedimientos de recuperación y respuesta.
- Cumplimiento normativo (ISO/IEC 27001, IEC 62443, NIST CSF).

A diferencia de la seguridad perimetral tradicional, basada en un único punto de control (por ejemplo, un firewall), la arquitectura anterior contempla que el atacante puede superar la

primera línea de defensa, por lo que deben existir mecanismos internos de detección, contención y mitigación.

Integración con Marcos Normativos y Técnicos

La arquitectura propuesta está alineada con múltiples marcos internacionales de seguridad, tales como:

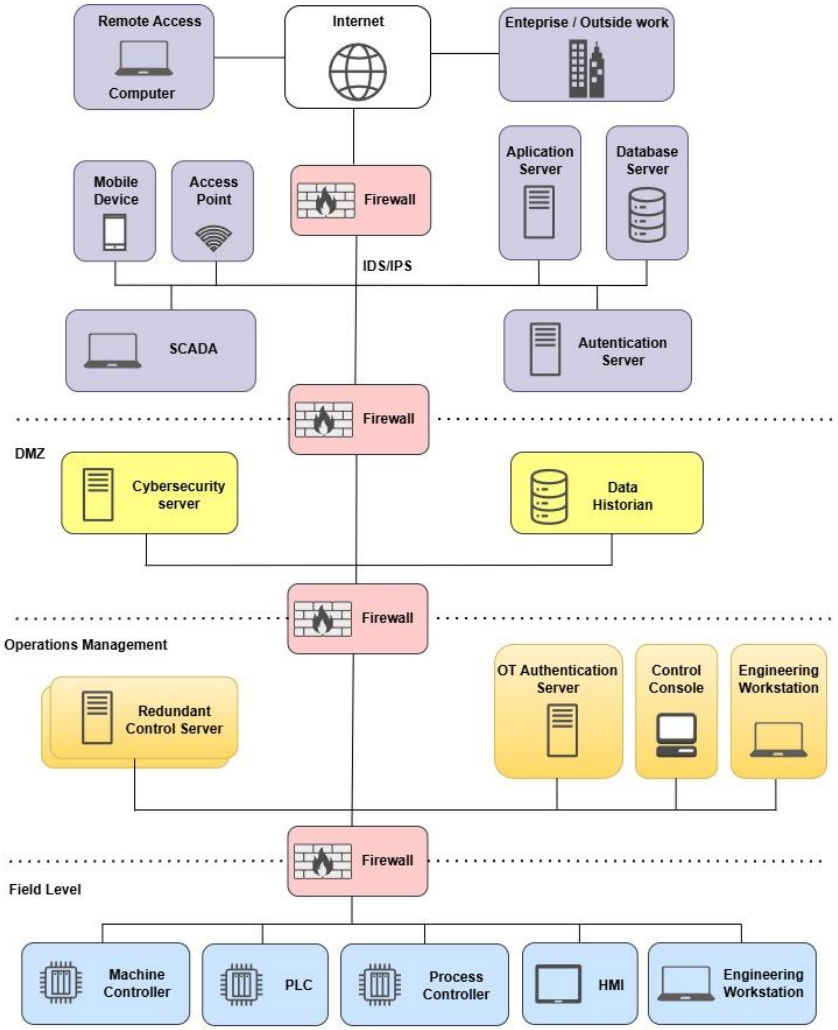
- IEC 62443-3-3, que propone requisitos de seguridad por niveles y zonas.
- NIST SP 800-82, que promueve la separación de redes, autenticación fuerte y monitoreo continuo.
- ISO/IEC 27001, con su enfoque basado en riesgos y mejora continua.

Las estrategias propuestas deben ser acompañadas por programas de concienciación para el personal operativo, auditorías regulares y revisiones de políticas de seguridad. También se debe considerar la madurez organizacional y la cultura de seguridad como factores clave en la adopción efectiva de estas medidas.

A continuación, presentamos un ejemplo de arquitectura basada en el principio de defensa en profundidad propuesta por la NIST SP 800-82R3.

Figura 9

Arquitectura Basada En Defensa en Profundidad



Nota. Arquitectura Basada en Guide to Operational Technology (OT) Security.

La arquitectura propuesta se basa en la segmentación de red por niveles, siguiendo el modelo Purdue, como parte de una estrategia de defensa en profundidad. Los dispositivos del nivel de campo (niveles 0-2) se aíslan de los sistemas de gestión de operaciones (nivel 3) y estos, a su vez, se separan de la red empresarial (nivel 4) mediante una Zona Desmilitarizada (DMZ). Todo tráfico entre IT y OT debe pasar por la DMZ, la cual debe estar protegida y monitoreada (Stouffer et al., 2023).

Se utilizan firewalls industriales entre zonas para controlar las comunicaciones, aplicando reglas para restringir el tráfico solo a lo autorizado. Además, se recomienda separar los servidores de autenticación para usuarios IT y OT.

En las capas de seguridad de hardware y software, se aplica el principio de mínima funcionalidad, deshabilitando servicios y puertos no necesarios (como servidores web o SSH en PLCs o HMIs) para reducir el riesgo de explotación.

Recomendaciones

Con base en los hallazgos obtenidos en este trabajo de grado, se proponen las siguientes recomendaciones con el fin de mitigar las vulnerabilidades y amenazas emergentes en los niveles de control y supervisión de los sistemas de control industrial (ICS):

Adoptar un Modelo de Seguridad por Capas

Es importante implementar una arquitectura de seguridad por capas que contemple controles físicos, lógicos y organizativos, tal como lo propone la norma IEC 62443. Esta estrategia debe incluir la segmentación de redes, el uso de firewalls industriales y la limitación del tráfico entre zonas OT e IT.

Actualizar y Proteger Tecnologías Obsoletas

Muchos entornos industriales dependen de sistemas antiguos que carecen de medidas de seguridad básicas. Se recomienda establecer políticas de gestión de activos que incluyan la identificación, actualización, aislamiento o virtualización de estos sistemas para reducir su exposición a amenazas externas.

Implementar un Programa de Gestión de Vulnerabilidades y Parches

Es necesario establecer un proceso periódico y controlado para evaluar, priorizar y aplicar actualizaciones de seguridad, considerando la criticidad de los activos y la posibilidad de realizar pruebas previas en entornos de laboratorio antes de su aplicación en producción.

Fortalecer el Monitoreo y la Detección de Amenazas

Se recomienda implementar soluciones de monitoreo industrial como IDS/IPS adaptados a protocolos OT, sistemas SIEM y tecnologías de análisis de comportamiento que permitan una respuesta temprana ante eventos anómalos o incidentes de seguridad.

Capacitar continuamente al Personal Operativo y Técnico

El factor humano sigue siendo una de las principales puertas de entrada para ataques cibernéticos. Por esto, es clave desarrollar programas de concienciación y formación periódica que permitan al personal identificar amenazas, aplicar buenas prácticas y actuar adecuadamente ante incidentes.

Elaborar y Mantener Planes de Respuesta Ante Incidentes

Las organizaciones deben contar con planes documentados de respuesta y recuperación ante incidentes cibernéticos que incluyan procedimientos técnicos, roles definidos y mecanismos de comunicación eficientes para minimizar el impacto de un ataque y restaurar rápidamente las operaciones.

Alinear las Prácticas de Seguridad con Marcos Normativos y Regulatorios

Se recomienda adoptar estándares reconocidos como IEC 62443, NIST SP 800-82, e ISO/IEC 27001, ajustando las políticas internas a estos marcos para asegurar una gestión integral y sistemática de los riesgos cibernéticos en entornos industriales.

Impacto del Proyecto en el Contexto de la Especialización

Este proyecto representa una contribución significativa al fortalecimiento del conocimiento especializado en el ámbito de la seguridad informática ya que permite aplicar y contextualizada los conceptos, marcos normativos y metodologías aprendidas a lo largo del programa académico. A través del análisis de vulnerabilidades y amenazas emergentes en sistemas de control industrial (ICS).

Desde el punto de vista académico, se trató de alinear el proyecto con los objetivos formativos de la especialización al abordar un problema real y vigente en el campo de la ciberseguridad y proponer estrategias de mitigación fundamentadas en estándares internacionales como el NIST SP 800-82 y la IEC 62443. Además, el desarrollo de instrumentos prácticos como checklists, cuestionarios de madurez y manuales de buenas prácticas permitió sintetizar y transferir el conocimiento.

Conclusiones

El desarrollo de este trabajo de grado permitió evidenciar que los sistemas de control industrial (ICS), en particular los niveles de control y supervisión definidos en la pirámide CIM, enfrentan un creciente número de vulnerabilidades y amenazas cibernéticas que comprometen seriamente la integridad, disponibilidad y confiabilidad de infraestructuras críticas. A través del análisis detallado de componentes como los PLC, SCADA, DCS y las redes industriales, se identificaron múltiples debilidades técnicas y estructurales que pueden ser explotadas por atacantes, afectando la operación de sectores estratégicos como la energía, el transporte, el agua y la manufactura.

Uno de los hallazgos más relevantes es que la mayoría de los ICS continúan operando con tecnologías obsoletas, configuraciones predeterminadas inseguras y protocolos de comunicación sin cifrado, factores que los convierten en blancos altamente vulnerables ante ataques dirigidos. La convergencia entre IT y OT, aunque representa una oportunidad para mejorar la eficiencia y el control operacional, también ha ampliado la superficie de ataque, permitiendo el movimiento lateral de amenazas desde redes corporativas hacia entornos industriales.

A través de casos de estudio y referencias normativas como la IEC 62443 y el marco NIST SP 800-82, se pudo constatar que muchas de las vulnerabilidades documentadas han sido explotadas en escenarios reales, causando pérdidas económicas significativas, interrupciones de servicios y riesgos para la seguridad pública. De la misma forma, se demostró que las amenazas emergentes, como el ransomware industrial, el malware avanzado dirigido a sistemas de automatización y la explotación de dispositivos IoT mal configurados, están en aumento y evolucionan constantemente.

Frente a este panorama, se concluye que la implementación de estrategias de mitigación es indispensable para la protección de los ICS. Entre las principales medidas identificadas se destacan la segmentación de redes, la gestión de parches, la aplicación de controles de acceso físico y lógico, el monitoreo constante y la capacitación del personal operativo. Además, se reafirma la importancia de adoptar una arquitectura de defensa en capas que considere no solo los aspectos tecnológicos, sino también organizativos y humanos.

Este estudio demuestra la necesidad de una mayor conciencia institucional y normativa respecto a la seguridad de los sistemas industriales. La protección de estos entornos no debe ser una opción, sino un requisito estratégico para garantizar la continuidad de los servicios esenciales de los que depende el funcionamiento de la sociedad moderna.

Referencias Bibliográficas

Adeyanju, I. A., Emake, E. D., Olaniyan, O. M., Omidiora, E. O., Adefarati, T., Uzedhe, G. O., & Okomba, N. S. (2021). Digital industrial control systems: Vulnerabilities and security technologies. *Current Applied Science and Technology*, *21*(1), 188–207. https://doi.org/10.14456/cast.2021.18

Agency, A. C. D. A. (2021). *DarkSide Ransomware: Best Practices for Preventing Business Disruption*. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a

Al Ghazo, A. T., & Kumar, R. (2024). ANDVI: Automated Network Device and Vulnerability Identification in SCADA/ICS by Passive Monitoring. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *54*(4), 2539–2550. https://doi.org/10.1109/TSMC.2023.3345254

Alqudhaibi, A., Albarrak, M., Aloseel, A., Jagtap, S., & Salonitis, K. (2023). Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations. *Sensors*, *23*(9). https://doi.org/10.3390/s23094539

American´s Cyber Defence Agency. (2025). *Cybersecurity Alerts & Advisories*. https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A95

Andreeva, O., Gordeychik, S., Gritsai, G., Kochetova, O., Potseluevskaya, E., Sidorov, S. I., & Timorin, A. A. (2016). Industrial Control Systems Vulnerabilities Statistics. *Kaspersky Lab, Report*, 19. https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

Anton, S. D. D., Fraunholz, D., Krohmer, D., Reti, D., Schneider, D., & Schotten, H. D. (2021).

The Global State of Security in Industrial Control Systems: An Empirical Analysis of Vulnerabilities around the World. *IEEE Internet of Things Journal*, *8*(24), 17525–17540. https://doi.org/10.1109/JIOT.2021.3081741

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges. *Internet of Things and Cyber-Physical Systems*, *4*(October 2023), 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

Cherepanov, A. (2017). WIN32/INDUSTROYER: A new threat for industrial control systems. *Eset*, 17. https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf

Cherepanov, A., & Lipovsky, R. (2017). *Industroyer: La mayor amenaza para los sistemas de control industrial desde Stuxnet*. Welivesecurity. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/

Conti, M., Donadel, D., & Turrin, F. (2021). A Survey on Industrial Control System Testbeds and Datasets for Security Research. *IEEE Communications Surveys and Tutorials*, *23*(4), 2248–2294. https://doi.org/10.1109/COMST.2021.3094360

Cusimano, J. (2022). Industrial control system risk assessment standards and leading practices in the chemical industry. *Process Safety Progress*, *41*(4), 665–669. https://doi.org/10.1B/prs.12372

CVE. (2025). *Common Vulnerabilities and Exposures*. https://www.cve.org/

Damayanthy, Y., Anaya, S., Tamaulipas, M., Tamaulipas, M., & Tamaulipas, M. (2022). El

impacto del internet de todas las cosas (IoT) en la vida cotidiana. *Ciencia Latina Revista Científica Multidisciplinar*, *6*(2), 1369–1378. https://doi.org/10.37811/cl_rcm.v6i2.1959

Djebbar, F., & Nordstrom, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, *11*(July), 85315–85332. https://doi.org/10.1109/ACCESS.2023.3303205

Dragos. (2023). *ICS Cybersecurity Year In Review 2022*. 70. https://www.dragos.com/year-in-review%0Ahttps://www.bing.com/images/search?q=ics+kill+chain&qpvt=ics+kill+chain&form=IGRE&first=1%0Ahttps://www.yokogawa.com/eu/blog/renewables/en/anatomy-cyber-attack-1/%0Ahttps://www.linkedin.com/pulse/you-aware-ics-kill-

Dragos. (2025). *2 0 2 5 OT/ICS CYBER SE CURIT Y REPORT*.

Duo, W., Zhou, M. C., & Abusorrah, A. (2022). A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. *IEEE/CAA Journal of Automatica Sinica*, *9*(5), 784–800. https://doi.org/10.1109/JAS.2022.105548

Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. Stuxnet Dossier, Symantec Security Response, Version 1.4, February 2011. *Symantec Security Response*, *4*(February), 1–69.

Firoozjaei, M. D., Mahmoudyar, N., Baseri, Y., & Ghorbani, A. A. (2022). An evaluation framework for industrial control system cyber incidents. *International Journal of Critical Infrastructure Protection*, *36*(May 2021), 100487. https://doi.org/10.1016/j.ijcip.2021.100487

Gauchi Risso, V. (2017). Estudio de los métodos de investigación y técnicas de recolección de datos utilizadas en bibliotecología y ciencia de la información. *Revista Espanola de*

Documentacion Cientifica, *40*(2), 1–13. http://redc.revistas.csic.es/index.php/redc/article/view/979/1503

Gawazah, L. (2024). To Pay or Not to Pay- The US Colonial Pipeline Ransomware Attack. *Researchgate*, *August*. https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack

Hollerer, S., Sauter, T., & Kastner, W. (2022). Risk Assessments Considering Safety, Security, and Their Interdependencies in OT Environments. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3538969.3543814

Hotellier, E., Sicard, F., Francq, J., & Mocanu, S. (2024). Standard specification-based intrusion detection for hierarchical industrial control systems. *Information Sciences*, *659*(March 2023), 120102. https://doi.org/10.1016/j.ins.2024.120102

Juan Sáenz Idoate, & Pedro Julián Becerril. (2023). *Ciberseguridad del PLC Siemens Simatic S7-300*.

Khan, R., Maynard, P., McLaughlin, K., Laverty, D., & Sezer, S. (2016). *Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid*. *2016*, 53–63. https://doi.org/10.14236/ewic/ics2016.7

Khan, S., & Madnick, S. E. (2021). Cybersafety: A System-theoretic Approach to Identify Cyber-vulnerabilities & Mitigation Requirements in Industrial Control Systems. *IEEE Transactions on Dependable and Secure Computing*, *19*(5), 3312–3328. https://doi.org/10.1109/TDSC.2021.3093214

Makrakis, G. M., Kolias, C., Kambourakis, G., Rieger, C., & Benjamin, J. (2021). Vulnerabilities and Attacks Against Industrial Control Systems and Critical Infrastructures. *Computer Science*, 1–40.

Mesbah, M., Elsayed, M. S., Jurcut, A. D., & Azer, M. (2023). Analysis of ICS and SCADA Systems Attacks Using Honeypots. *Future Internet*, *15*(7). https://doi.org/10.3390/fi15070241

Mestre, H. R. (2018). *Ciberseguridad en Sistemas de Control Industrial o ICSs*.

Muller, N., Ziras, C., & Heussen, K. (2022). Assessment of Cyber-Physical Intrusion Detection and Classification for Industrial Control Systems. *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, SmartGridComm 2022*, *91363*, 432–438. https://doi.org/10.1109/SmartGridComm52983.2022.9961010

NIST. (2025). *National Vulnerability Database*. https://nvd.nist.gov/

Pal, R., Liu, P., Lu, T., & Hua, E. (2023). How Hard Is Cyber-risk Management in IT/OT Systems? A Theory to Classify and Conquer Hardness of Insuring ICSs. *ACM Transactions on Cyber-Physical Systems*, *6*(4). https://doi.org/10.1145/3568399

Pancho, G., & Galarza, F. (2014). Formulación de un Marco de Referencia de Convergencia IT/OT. *Revista Técnica "Energía," 10*(1), 208–214. https://doi.org/10.37116/revistaenergia.v10.n1.2014.117

Pinto, A. Di, Dragoni, Y., & Carcano, A. (2018). TRITON: The First ICS Cyber Attack on Safety Instrument Systems Understanding the Malware, Its Communications and Its OT Payload. *Black Hat USA 2018*.

https://scadahacker.com/library/Documents/Cyber_Events/Nozomi - TRITON - The First SIS Cyberattack.pdf

Quiroz Tascón, S., Zapata Jiménez, J., & Vargas Montoya, H. F. (2020). Predicción de ciberataques en sistemas industriales SCADA a través de la implementación del filtro Kalman. *TecnoLógicas*, *23*(48), 249–267. https://doi.org/10.22430/22565337.1586

Ryu, D., Lee, S., Yang, S., Jeong, J., Lee, Y., & Shin, D. (2024). Enhancing Cybersecurity in Energy IT Infrastructure Through a Layered Defense Approach to Major Malware Threats. *Applied Sciences (Switzerland)*, *14*(22). https://doi.org/10.3390/app142210342

Stouffer, K., Zimmerman, T., Stouffer, K., & Zimmerman, T. (2023). *Guide to Operational Technology (OT) Security*. *September*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-82r3

Trend Micro. (2022). *Informe anual de ciberseguridad de 2021 de Trend Micro*. https://www.trendmicro.com/vinfo/es/security/research-and-analysis/threat-reports/roundup/navigating-new-frontiers-trend-micro-2021-annual-cybersecurity-report

Weiss, J., Stephens, R., Miller, N., & Michael, J. B. (2022). Control System Cyber Incidents Are Real - And Current Prevention and Mitigation Strategies Are Not Working. *Computer*, *55*(1), 128–137. https://doi.org/10.1109/MC.2021.3124359

Zanasi, C., Magnanini, F., Russo, S., & Colajanni, M. (2022). A Zero Trust approach for the cybersecurity of Industrial Control Systems. *NCA 2022 - 2022 IEEE 21st International Symposium on Network Computing and Applications*, *21*, 1–7. https://doi.org/10.1109/NCA57778.2022.10013559

Zare, F., Mahmoudi-Nasr, P., & Yousefpour, R. (2024). A real-time network based anomaly detection in industrial control systems. *International Journal of Critical Infrastructure Protection*, *45*(December 2023), 100676. https://doi.org/10.1016/j.ijcip.2024.100676

Apéndices

Con el fin de complementar y fortalecer los hallazgos obtenidos en el presente trabajo de grado, se han desarrollado una serie de Apéndices prácticos que tienen como propósito servir de guía, diagnóstico y apoyo técnico para organizaciones interesadas en mejorar su postura de ciberseguridad en entornos industriales.

Los Apéndices presentados permiten traducir el conocimiento teórico y normativo abordado en el estudio hacia herramientas concretas de aplicación que pueden ser utilizadas tanto por responsables técnicos de sistemas OT como por gestores de riesgos o auditores de seguridad.

Apéndice A Checklist de buenas prácticas en ciberseguridad para sistemas de control industrial: permite realizar una evaluación rápida y estructurada del estado de seguridad en componentes críticos de los sistemas industriales, facilitando la identificación de brechas o debilidades

Apéndice B Cuestionario de madurez en ciberseguridad OT: proporciona una herramienta para valorar el nivel de madurez de la organización en términos de gobernanza, políticas, controles técnicos y cultura de ciberseguridad, utilizando un enfoque escalonado que permite orientar planes de mejora.

Apéndice C Manual de buenas prácticas en ciberseguridad para ICS: ofrece recomendaciones prácticas y priorizadas, basadas en normas internacionales como la IEC 62443 y el NIST SP 800-82, para fortalecer la seguridad en los niveles de supervisión y control de la pirámide CIM.

En conjunto, estos Apéndices representan un aporte metodológico que busca ir más allá del diagnóstico académico, promoviendo la implementación de medidas concretas que

contribuyan a proteger los sistemas de control industrial frente a amenazas actuales y emergentes.

Apéndice A

Checklist de Buenas Prácticas en Ciberseguridad para Sistemas de Control Industrial

Este checklist tiene como objetivo servir como herramienta de autoevaluación para organizaciones industriales que operan sistemas de control. Está dividido en secciones clave de la seguridad OT y permite verificar el nivel de cumplimiento de buenas prácticas esenciales.

Marcar "**Sí**", "**Parcial**" o "**No**" según corresponda y utilizar el campo de observaciones para comentarios específicos.

1. Segmentación de redes

Pregunta	Sí	Parcial	No
¿Existe separación entre la red de IT y la red OT?			
¿Se utilizan VLANs o zonas industriales lógicas?			
¿Hay firewalls industriales con reglas específicas entre zonas?			
¿Existe una DMZ entre las redes externas y la red de control?			
¿Se monitorea el tráfico entre zonas críticas?			

Observaciones:

_____

2. Gestión de parches y vulnerabilidades

Pregunta	Sí	Parcial	No
¿Se cuenta con un inventario actualizado de activos OT?			
¿Se consultan boletines de vulnerabilidades ICS de forma regular?			
¿Se prueban los parches en entornos controlados antes de aplicarlos?			
¿Se aplican controles compensatorios cuando no es posible parchear?			

¿Existe un procedimiento documentado para gestión de actualizaciones?			

Observaciones:

---

3. Control de acceso físico y lógico

Pregunta	Sí	Parcial	No
¿Las salas de control y gabinetes están físicamente restringidos?			
¿Se utilizan tarjetas, PIN o biometría para acceso físico?			
¿Los usuarios cuentan con privilegios mínimos necesarios (RBAC)?			
¿Existe autenticación multifactor (MFA) para accesos remotos?			
¿Se auditan y registran los accesos a sistemas críticos?			

Observaciones:

---

4. Monitoreo y detección

Pregunta	Sí	Parcial	No
¿Existe un IDS o sistema de monitoreo en red OT?			
¿Se analizan los eventos de seguridad con herramientas SIEM?			
¿Hay alertas configuradas para tráfico inusual o acceso no autorizado?			
¿Se realizan revisiones periódicas de logs y actividad del sistema?			

Observaciones:

---

5. Cultura organizacional y concienciación

Pregunta	Sí	Parcial	No
¿El personal recibe capacitación periódica en ciberseguridad OT?			
¿Existen campañas de concienciación sobre ingeniería social?			
¿Hay procedimientos de respuesta ante incidentes documentados?			
¿Se realizan simulacros de incidentes o ejercicios de respuesta?			
¿Existe un comité o responsable de seguridad OT definido?			

Observaciones:

Apéndice B

Cuestionario De Madurez en Ciberseguridad para Entornos OT

Este cuestionario tiene como objetivo evaluar el nivel de madurez en ciberseguridad de entornos OT, considerando estándares como IEC 62443, NIST CSF y ISO/IEC 27001. Se basa en una escala de 0 a 5, donde 0 es 'No implementado' y 5 'Optimizado'. Permite identificar brechas, priorizar mejoras y establecer planes de acción.

Escala de madurez

0. No implementado: No hay controles ni procedimientos.

1. Inicial: Reconocimiento informal de la necesidad.

2. Repetible: Controles aplicados de forma no estandarizada.

3. Definido: Procesos documentados y comunicados.

4. Gestionado: Revisión y mejora basada en indicadores.

5. Optimizado: Mejora continua, automatización y auditoría periódica.

A continuación, se presenta un ejemplo para la implementación del cuestionario.

Ejemplo del Cuestionario.

Nivel	Descripción	Ejemplo
0. No implementado	No hay controles ni procedimientos.	No existe política de acceso o inventario de activos.
1. Inicial	Reconocimiento informal de la necesidad.	Se comentan riesgos, pero no hay procesos definidos.
2. Repetible	Controles aplicados de forma no estandarizada.	Se aplican parches, pero sin plan documentado.
3. Definido	Procesos documentados, conocidos y comunicados.	Hay política de seguridad OT y responsables asignados.

4. Gestionado	Se revisan y miden los procesos implementados.	Auditorías internas periódicas, revisión de métricas.
5. Optimizado	Se aplican mejoras continuas y automatización.	Uso de dashboards OT, respuesta automática ante anomalías.

1. **Gobernanza y gestión estratégica**

¿Existe una política formal de ciberseguridad OT, firmada por la dirección?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se han definido roles y responsabilidades específicas para OT?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Está la seguridad OT integrada en la estrategia de la organización?

Nivel de madurez (0-5): _____

Observaciones:

_____

2. **Gestión de activos y vulnerabilidades**

¿Se mantiene un inventario detallado de equipos, firmware y software industrial?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se realiza escaneo regular de vulnerabilidades en la red OT?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se aplican parches de seguridad según una política definida y con pruebas previas?

Nivel de madurez (0-5): _____

Observaciones:

_____

3. Control de accesos y autenticación

¿Se aplica RBAC en sistemas SCADA, HMI y servidores OT?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se usa MFA para accesos remotos o críticos?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se auditan los accesos y se gestionan cuentas inactivas?

Nivel de madurez (0-5): _____

Observaciones:

_____

4. Segmentación y comunicaciones seguras

¿Está segmentada la red OT de la red IT (mediante DMZ, firewalls o VLANs)?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se utilizan zonas y conductos según IEC 62443?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿El tráfico OT cuenta con filtrado y cifrado apropiado?

Nivel de madurez (0-5): _____

Observaciones:

_____

5. Monitoreo, detección y respuesta

¿Se utilizan sensores de red o IDS industriales para monitoreo de tráfico?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Existe un plan de respuesta a incidentes OT documentado y probado?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se han realizado ejercicios o simulacros con personal OT?

Nivel de madurez (0-5): _____

Observaciones:

_____

6. Concienciación y cultura de seguridad

¿El personal OT recibe capacitación anual en ciberseguridad?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Se ejecutan campañas sobre amenazas comunes como phishing o USB maliciosos?

Nivel de madurez (0-5): _____

Observaciones:

_____

¿Existe un canal interno de reporte de incidentes accesible para operarios?

Nivel de madurez (0-5): _____

Observaciones:

_____

Interpretación sugerida

• Niveles 0–2: Requiere intervención prioritaria (riesgo alto).

• Niveles 3–4: Buen nivel, con oportunidades de mejora estructurada.

• Nivel 5: Madurez avanzada. Se recomienda mantener prácticas de mejora continua.

Apéndice C

Manual de buenas prácticas en ciberseguridad para ICS

1. **Segmentación de redes (IEC 62443-3-2, NIST SP 800-82)**

Objetivo: Limitar el movimiento lateral de atacantes y contener amenazas dentro de zonas delimitadas.

Buenas prácticas:

- Clasificar la red OT en zonas de seguridad según funciones y niveles de riesgo (por ejemplo, producción, supervisión, administración).
- Utilizar firewalls industriales con inspección de protocolos OT (Modbus, DNP3, OPC UA).
- Crear conductos seguros (conduits) entre zonas con control de tráfico, autenticación y cifrado, según IEC 62443.
- Ubicar los servidores SCADA en una DMZ, sin acceso directo desde internet ni desde la red IT.
- Aplicar listas de control de acceso (ACLs) en switches y routers industriales.
- Implementar firewalls lógicos entre estaciones de ingeniería y PLCs.

Ejemplo:

Una red de subestación eléctrica que segmenta el IED, HMI y gateway de datos por VLANs separadas con firewalls L2.

2. **Gestión de parches y vulnerabilidades (IEC 62443-2-1, NIST CSF-ID.RA-1)**

Objetivo: Reducir la exposición a amenazas conocidas mediante parches, actualizaciones y controles compensatorios.

Buenas prácticas:

- Realizar análisis de impacto operacional antes de aplicar actualizaciones (compatibilidad de firmware, interrupciones de proceso).
- Utilizar herramientas como Nessus, Qualys, OpenVAS o SCAP para escaneo de vulnerabilidades y auditorías periódicas.

- Establecer una política de parches documentada que defina periodicidad, roles, entornos de prueba y registro.
- Identificar y gestionar activos no actualizables (legacy) con segmentación estricta, control de acceso y monitoreo pasivo.
- Configurar servidores de actualización internos para firmware o software aprobado (en red OT sin conexión directa a internet).

Ejemplo:

Una empresa química mantiene servidores de control aislados y aplica parches solo luego de simularlos en un laboratorio OT.

3. **Control de acceso físico y lógico (IEC 62443-3-3, ISO 27002:2022 A.9)**

Objetivo: Prevenir accesos no autorizados a dispositivos, redes y datos críticos.

Buenas prácticas:

- Asegurar salas de servidores, tableros eléctricos y zonas críticas con control de ingreso electrónico y videovigilancia.
- Implementar autenticación multifactor (MFA) para accesos remotos y tareas de administración.
- Configurar RBAC (Role-Based Access Control) en sistemas SCADA/HMI, limitando el acceso según función: operador, supervisor, ingeniero, auditor.
- Bloquear cuentas inactivas, deshabilitar usuarios predeterminados y renombrar nombres por defecto (admin, root, etc.).
- Auditar cambios de configuración mediante bitácoras centralizadas o SIEM, con alertas para acciones no autorizadas.

Ejemplo:

Un sistema de planta usa tarjetas RFID para entrar a la sala SCADA y MFA para acceso remoto a sus HMI virtualizadas.

4. **Monitoreo y detección de incidentes (IEC 62443-2-4, NIST SP 800-94)**

Objetivo: Detectar actividades anómalas o maliciosas en la red y responder tempranamente.

Buenas prácticas ampliadas:

- Desplegar sensores IDS/IPS (Intrusion Detection System/Intrusion Prevention System) industriales compatibles con protocolos OT.
- Monitorear logs de switches, PLCs, firewalls y estaciones SCADA usando SIEM como Wazuh, Splunk, Qradar o Elastic Stack.
- Analizar patrones de tráfico con herramientas de detección basada en comportamiento UBA/NBA (User Behavior Analytics/Network Behavior Analytics).

  Configurar alertas por:

  - Cambios de configuración no autorizados.
  - Escaneos de red.
  - Comunicación con direcciones externas inusuales.
- Revisar periódicamente alertas y realizar retrospectiva de eventos después de cada incidente.

  Ejemplo:

  Una refinería detectó intentos de escaneo de Modbus TCP con Zeek, activando un plan de respuesta y bloqueando el segmento.

5. Concienciación y formación (ISO/IEC 27001:2022 A.7 y A.6.3.1)

Objetivo: Involucrar al personal técnico y operativo en la cultura de ciberseguridad.

Buenas prácticas ampliadas:

- Capacitar al personal sobre:
  - Reconocimiento de ingeniería social.
  - Manejo de dispositivos USB.
  - Normas de seguridad de red.

- Simular incidentes:
  - Correos tipo phishing.
  - Accesos no autorizados.
  - Fallos de comunicación en red OT.

- Establecer un canal interno de reporte de incidentes accesible.
- Designar embajadores de ciberseguridad por área, encargados de reforzar prácticas seguras.

Ejemplo:

Una empresa minera realiza simulacros cada trimestre, involucrando a operadores de campo, ingenieros y personal de TI.

6. **Integración con normativas y marcos de referencia**

Objetivo: Alinear la estrategia de ciberseguridad con estándares internacionales y regulaciones sectoriales.

Estándares clave:

- IEC 62443: Estandariza la seguridad por capas en entornos industriales.
- NIST SP 800-82: Guía específica para ICS en entornos estadounidenses.
- ISO/IEC 27001: Gestión de seguridad de la información aplicable a TI/OT.
- NIST CSF: Enfoque por funciones (Identificar, Proteger, Detectar, Responder, Recuperar).

Apéndice D

Glosario

Amenaza cibernética: Evento o acción maliciosa que busca explotar vulnerabilidades en un sistema para causar daño, interrupción o acceso no autorizado.

APT (Amenaza Persistente Avanzada): Amenaza cibernética sofisticada y prolongada, comúnmente asociada a actores con altos recursos (gubernamentales o privados), que buscan infiltrarse y permanecer ocultos en sistemas críticos.

Automatización: Uso de sistemas o dispositivos para realizar tareas con mínima intervención humana, mejorando la eficiencia, precisión y repetitividad en procesos industriales.

Ciberhigiene: Conjunto de buenas prácticas rutinarias para proteger sistemas informáticos y datos, como actualizaciones periódicas, gestión de contraseñas y control de accesos.

Ciberseguridad industrial: Disciplina dedicada a proteger los sistemas de control industrial y las infraestructuras críticas frente a amenazas y riesgos cibernéticos.

Conduits: Canales definidos en la norma IEC 62443 que controlan la comunicación entre zonas segmentadas en una red industrial, con reglas específicas de seguridad.

Convergencia IT-OT: Integración entre las tecnologías de la información (IT) y las tecnologías operativas (OT), que permite una mayor eficiencia en la supervisión y control de procesos industriales, pero también incrementa la superficie de ataque.

Controles de acceso físico: Medidas de seguridad que restringen el acceso físico a áreas sensibles, salas de servidores o dispositivos industriales.

DCS (Sistema de Control Distribuido): Sistema de control utilizado en procesos industriales complejos, donde las funciones de supervisión y control están distribuidas en distintos dispositivos y ubicaciones dentro de la planta.

Defensa en profundidad: Estrategia de seguridad que implementa múltiples capas de defensa para proteger sistemas, permitiendo mitigar amenazas incluso si una capa falla.

DMZ (Zona Desmilitarizada): Segmento intermedio de red, comúnmente utilizado para exponer servicios públicos (como servidores SCADA) sin comprometer la red interna.

Firewall industrial: Dispositivo diseñado para proteger redes OT, capaz de filtrar tráfico de protocolos industriales específicos como Modbus, DNP3 o OPC UA.

Gestión de parches: Proceso continuo de evaluación, validación e instalación de actualizaciones para corregir vulnerabilidades y errores en sistemas y software.

HMI (Interfaz Hombre-Máquina): Herramienta visual que permite la interacción entre los operadores humanos y los sistemas de control, mostrando datos del proceso y permitiendo la emisión de comandos.

ICS (Sistemas de Control Industrial): Conjunto de dispositivos, redes y software utilizados para supervisar, controlar y automatizar procesos industriales en sectores críticos como energía, agua, manufactura o transporte.

IDS (Sistema de Detección de Intrusos): Herramienta que monitorea sistemas y redes para detectar actividades sospechosas o no autorizadas.

IIoT (Internet Industrial de las Cosas): Aplicación del Internet de las Cosas en entornos industriales, donde sensores y dispositivos inteligentes recolectan y transmiten datos para optimizar procesos y operaciones.

Infraestructura crítica: Conjunto de sistemas esenciales para el funcionamiento de una sociedad, como plantas eléctricas, redes de transporte, telecomunicaciones o suministro de agua potable.

IPS (Sistema de Prevención de Intrusos): Extensión del IDS que no solo detecta amenazas, sino que también actúa automáticamente para bloquear o mitigar ataques.

IT (Tecnologías de la Información): Conjunto de recursos tecnológicos (hardware, software, redes) utilizados para gestionar, procesar y almacenar información en una organización.

Modbus: Protocolo de comunicación ampliamente utilizado en sistemas de automatización industrial, conocido por su simplicidad, pero también por la falta de características de seguridad nativas.

OPC UA (Unified Architecture): Estándar de comunicación moderna y segura para intercambio de datos industriales, con soporte para cifrado, autenticación y control de acceso.

OT (Tecnologías Operativas): Sistemas y tecnologías utilizadas en el monitoreo y control de procesos físicos en entornos industriales, como sensores, PLCs y SCADA.

Phishing: Técnica de ingeniería social que busca engañar a una persona para que revele información confidencial, como contraseñas o datos financieros.

PLC (Controlador Lógico Programable): Dispositivo electrónico programable que ejecuta secuencias lógicas para controlar maquinaria industrial, actuadores y sensores en tiempo real.

SCADA (Sistema de Supervisión, Control y Adquisición de Datos): Sistema que permite supervisar y controlar procesos industriales a distancia, recopilando datos en tiempo real y gestionando alertas.

Segmentación de redes: Estrategia de seguridad que divide una red en zonas aisladas para limitar el movimiento lateral de los atacantes y contener posibles intrusiones.

SOC (Centro de Operaciones de Seguridad): Unidad especializada encargada de monitorizar, detectar, analizar y responder a incidentes de ciberseguridad en una organización.

Stuxnet: Malware descubierto en 2010, considerado uno de los primeros ciberataques a ICS. Infectó sistemas SCADA para sabotear centrifugadoras en una planta nuclear iraní, manipulando directamente PLCs

Superficie de ataque: Conjunto de todos los puntos potenciales por los cuales un sistema puede ser atacado o comprometido.

Vulnerabilidad: Debilidad en un sistema, protocolo o configuración que puede ser explotada por un atacante para causar daño, acceder a recursos o interrumpir el funcionamiento normal.

Zero Trust: Modelo de seguridad que parte del principio de “nunca confiar, siempre verificar”, donde todo acceso debe ser autenticado y monitoreado, incluso si proviene del interior de la red.