UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Propuesta de plan de seguridad informática para sistema de control industrial mediante lineamientos del Centro para la Seguridad de Internet
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Silva Alvarado Cristian Daniel
Tutor/a:
PhD. Maryory Urdaneta Herrera Mg. Renato Mauricio Toasa Guachi

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, **Maryory Urdaneta Herrera** con C.I: **1759316126** en mi calidad de Tutor del proyecto de investigación titulado: **Propuesta de plan de seguridad informática para sistema de control industrial mediante lineamientos del Centro para la Seguridad de Internet.**

Elaborado por: **Silva Alvarado Cristian Daniel**, de C.I: **2100352117**, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

_____

Firmas

APROBACIÓN DEL TUTOR

Yo, **Renato Mauricio Toasa Guachi** con C.I: **1804724167** en mi calidad de Tutor del proyecto de investigación titulado: **PROPUESTA DE PLAN DE SEGURIDAD INFORMÁTICA PARA SISTEMA DE CONTROL INDUSTRIAL MEDIANTE LINEAMIENTOS DEL CENTRO PARA LA SEGURIDAD DE INTERNET.** Elaborado por: **Silva Alvarado Cristian Daniel**, de C.I: **2100352117**, estudiante de la Maestría de Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Silva Alvarado Cristian Daniel con C.I: 2100352117, autor del proyecto de titulación denominado: **Propuesta de plan de seguridad informática para sistema de control industrial mediante lineamientos del Centro para la Seguridad de Internet.** Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

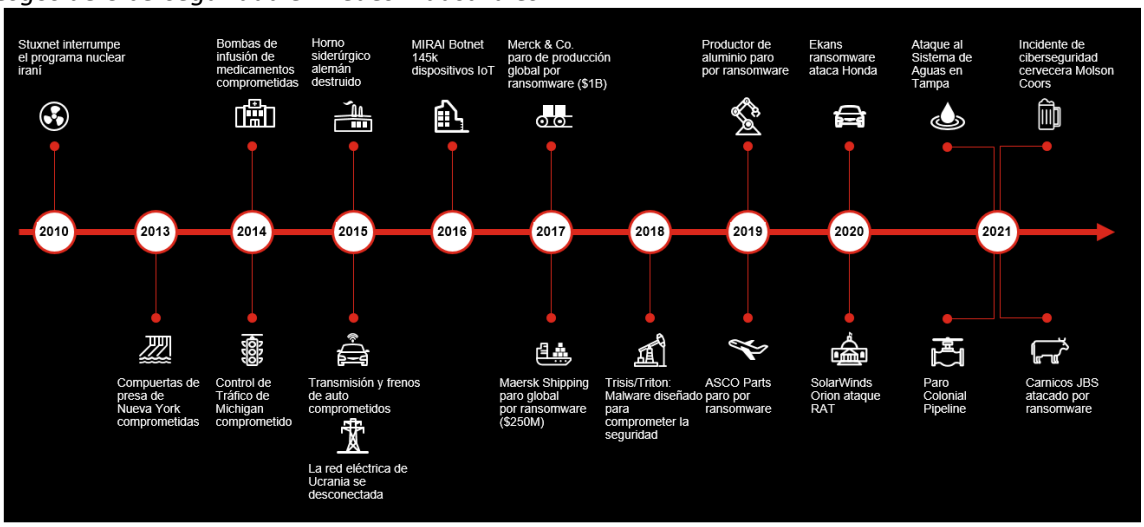
INFORMACIÓN GENERAL

Contextualización del tema

En la actualidad existen diversos riesgos relacionados con ciberseguridad en las redes industriales. Los ataques cibernéticos crecen en frecuencia y en impacto, provocando pérdidas millonarias a diversas industrias a nivel mundial sin importar cual sea su actividad empresarial, se detalla su evolución en la **Figura 1**.

Figura 1

Riesgos de Ciberseguridad en Redes Industriales



En el año 2023, Ecuador ratificó su compromiso con los objetivos de desarrollo sostenible como una política del Gobierno nacional. Este compromiso ha sido tomado en cuenta por el sector privado y la sociedad civil con la premisa de lograr los objetivos en común.

Una empresa dedicada a la minería que tiene una sede importante ubicada en el sur del Ecuador, analiza el uso de los Controles de Seguridad Críticos (CSC) del Centro para la Seguridad del Internet (CIS) en entornos de tecnología operativa (OT), ya que es una práctica cada vez más común en la industria para temas de seguridad. Los CIS son una lista priorizada de controles de seguridad cibernética, que se han adaptado para ser usadas en sistemas de control industrial. A continuación, se presentan algunos antecedentes que contextualizan el uso de CIS en entornos OT:

El documento CIS Controls para sistemas de control industrial, proporciona una guía y una descripción general de los controles y cómo se pueden aplicar en entornos OT (Gary, 2018).

(Morgan, 2020), los CIS Controls pueden ayudar a los profesionales de la seguridad a construir la base de un programa sólido de ciberseguridad OT. El artículo destaca la importancia de la priorización y la implementación de los controles en grupos digeribles

Este trabajo de investigación analiza la ciberseguridad industrial y propone una arquitectura de referencia de seguridad para entornos industriales, basada en estándares del sector como el IEC 62443. El trabajo destaca la importancia de la segmentación de red y la defensa en profundidad en entornos OT (Mendoza, 2021).

Oportunidades y desafíos para el desarrollo productivo de la provincia de Santa Fe: Este trabajo de investigación analiza la automatización y la robótica en la sociedad y cómo afecta a la productividad, el empleo, los salarios, la formación y la investigación. El trabajo destaca la importancia de la ciberseguridad en la industria 4.0 y cómo los CIS Controls pueden ayudar a proteger los sistemas de información (Erbes et al., 2019).

En el Webinar "La Seguridad en Entornos IT / OT" se discute la convergencia de IT/OT y cómo los CIS Controls pueden ayudar a proteger los sistemas de información en entornos OT. El Webinar destaca la importancia de la segmentación de red y la defensa en profundidad en entornos OT (Factory, 2019).

Debido al crecimiento y las necesidades actuales de la industria y las tecnologías de la información, las empresas ahora tienen incorporados a su inventario, varios equipos que pueden quedar vulnerables en el caso de que no exista una infraestructura y políticas de seguridad confiables para mantenerlos al margen de cualquier intrusión.

El presente plan, dará una pauta para cualquier especialista en seguridad informática acerca de cómo lograr abordar varios de los temas más importantes que hay que tener en cuenta al momento de evaluar la seguridad en redes de tecnología operativa de diversos tipos de industrias, ya que, si bien es cierto se habla de una empresa minera, la metodología y herramientas pueden ser usadas y acoplarse a la mayoría de las industrias.

Problema de investigación

En agosto de 2023, una empresa minera que se dedica a la extracción de oro, con sede en el sur de Ecuador, realizó una exhaustiva evaluación de seguridad en sus redes de control industrial (OT), debido a que requieren cumplir con diversas normas establecidas a nivel corporativo respecto a la seguridad sus redes. Esta iniciativa, impulsada por su compromiso con la seguridad y la eficiencia operacional, busca blindar su infraestructura crítica frente a las crecientes amenazas cibernéticas que podrían afectar sus operaciones. La interrupción de la producción debido a un ataque cibernético o un fallo en el sistema, puede ocasionar importantes pérdidas económicas e incluso la empresa podría enfrentar multas y sanciones por no cumplir con las normas y regulaciones necesarias.

Un especialista en seguridad informática, con amplia experiencia en el sector industrial, se trasladó a la mina durante una semana para realizar un análisis profundo del entorno OT. Para ello, se valió de sensores especializados de Nozomi Networks que capturaron información detallada sobre los

sistemas de red y seguridad, y recopilaron archivos de configuración de los sistemas de red y seguridad.

Fruto de la evaluación, se elaboró un detallado informe técnico que documenta todos los riesgos y vulnerabilidades detectados en la red de la empresa. Este informe servirá como base para la elaboración de un plan de seguridad informática que permita gestionarlos hallazgos.

Objetivo general

Elaborar una propuesta de un plan de seguridad informática, que aborde cada uno de los problemas identificados en las redes de control industrial de una empresa minera del Ecuador.

Objetivos específicos

- Realizar una contextualización de las herramientas, que permitan evaluar el entorno de tecnología operativa para identificar posibles vulnerabilidades y puntos de riesgo.
- Determinar la pauta que confirme el cumplimiento actual de los Controles de Seguridad Críticos del CIS.
- Diseñar un plan de seguridad informática, que permita clasificar las vulnerabilidades identificadas según su gravedad y potencial impacto en la seguridad del entorno OT, priorizando aquellas que representan mayores riesgos.
- Validar la propuesta de solución específica detallada en el plan, para cada una de las vulnerabilidades y riesgos identificados.

Vinculación con la sociedad y beneficiarios directos:

El desarrollo de plan de seguridad informático cumple con las metas del Objetivo de Desarrollo Sostenible número 9 “Industria, Innovación e Infraestructura” (Unidas, 2024).

Algunos de los principales beneficiarios directos son:

Organizaciones industriales: las organizaciones que operan SCI, se benefician de una mayor seguridad de sus sistemas, lo que reduce el riesgo de interrupción de la producción, daños a la propiedad y pérdidas financieras.

Gobierno: Los gobiernos tienen la responsabilidad de proteger la infraestructura crítica y la seguridad nacional. La propuesta de este plan ayuda a los gobiernos a cumplir con esta responsabilidad.

Ciudadanos: Los ciudadanos se benefician de una infraestructura crítica más segura y confiable, lo que significa que existe un menor riesgo de interrupción de servicios esenciales como la energía, el agua y el transporte.

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

No hay duda que las tecnologías de la información y las comunicaciones (TIC), respaldan la mayoría de los servicios que se prestan a nivel mundial en la actualidad. La humanidad aún cuenta con pocos servicios básicos, que no dependan de las tecnologías de la información para su normal funcionamiento. Esto llega en un momento de cambios a alta velocidad y es el resultado de los esfuerzos de eficiencia en todos los departamentos. En los últimos años, estos procesos de cambio han estado impulsados por iniciativas de transformación digital, que involucran a casi todas las organizaciones. La situación actual hará que la dependencia de la tecnología de la información, sea aún mayor en el futuro.

Un sistema de control industrial es un conjunto de hardware y software, que se utiliza para monitorear y controlar los procesos físicos, dispositivos y la infraestructura en entornos industriales. Los sistemas de control industrial pueden variar en tamaño y complejidad, desde unos pocos controladores modulares montados en panel, hasta grandes sistemas de control distribuidos interactivos e interconectados con muchos miles de conexiones de campo (Industrias, 2023).

La tecnología operativa (OT) es el uso de hardware y software para monitorear y controlar los procesos físicos, los dispositivos y la infraestructura en entornos industriales. La OT se utiliza en una diversidad de industrias, que incluyen la manufactura, el petróleo y gas, la generación y distribución eléctrica, la aviación, la marítima, la ferroviaria y los servicios públicos. La OT se contrapone con la tecnología de la información (TI), la cual se ocupa de los sistemas de datos y se utiliza principalmente para resolver problemas empresariales. Sin embargo, muchos aspectos de ambas tecnologías convergen, ya que los sistemas de la OT por lo general están conectados a las redes, y generan y utilizan volúmenes de datos cada vez mayores (Fortinet, 2023).

Según (Center for Internet Security, 2021) El Centro de Seguridad de Internet (CIS) es una organización sin fines de lucro que se dedica a mejorar la seguridad cibernética global a través de la colaboración, el desarrollo de mejores prácticas y la promoción de la educación en seguridad. Fundada en 2003, CIS se ha convertido en una de las organizaciones líderes en el campo de la seguridad cibernética, con un impacto significativo en organizaciones de todo el mundo.

Las principales actividades de CIS incluyen:

Desarrollo de los CIS Controls: Un conjunto de 20 recomendaciones de mejores prácticas para la seguridad cibernética, reconocido internacionalmente por su eficacia en la protección de organizaciones de diversos tamaños e industrias.

Publicación de informes y guías: CIS ofrece una amplia gama de recursos informativos sobre las últimas amenazas y tendencias en seguridad cibernética, ayudando a las organizaciones a mantenerse al día y tomar decisiones informadas.

Evaluación de riesgos y madurez: CIS proporciona herramientas y servicios para que las organizaciones puedan evaluar su postura de seguridad actual e identificar áreas de mejora.

Capacitación y educación: CIS ofrece una variedad de programas de capacitación y educación para profesionales de la seguridad cibernética, con el objetivo de aumentar el conocimiento y las habilidades en la materia.

Promoción de la colaboración público-privada: CIS trabaja con gobiernos, empresas y otras organizaciones para promover la colaboración y el intercambio de información en materia de seguridad cibernética.

Los principales beneficios de participar con CIS incluyen:

Mejora de la postura de seguridad: Implementar los CIS Controls y utilizar las herramientas y recursos de CIS, puede ayudar a las organizaciones a reducir significativamente el riesgo de ataques cibernéticos.

Reducción de costos: La inversión en seguridad cibernética, puede ayudar a las organizaciones a evitar los costos asociados con la recuperación de un ataque cibernético.

Aumento de la confianza: Implementar prácticas de seguridad sólidas, puede ayudar a las organizaciones a aumentar la confianza de sus clientes, socios y empleados.

Cumplimiento normativo: Los CIS Controls se alinean con las principales regulaciones de seguridad cibernética, lo que ayuda a las organizaciones a cumplir con los requisitos legales.

El Centro de Seguridad de Internet es un recurso invaluable para cualquier organización que busca mejorar su seguridad cibernética.

El CIS ha adaptado Los Controles de Seguridad Críticos (CSC) para sistemas de control industrial (CIS). Los CIS Controls son una lista priorizada de controles de seguridad cibernética que se han adaptado para su uso en SCI. Los CIS Controls pueden ayudar a proteger los sistemas de información en entornos OT y son especialmente valiosos en la industria 4.0 (Gary, 2018).

Los CSC del CIS son un conjunto de 18 controles de seguridad cibernética que se han desarrollado para ayudar a las organizaciones a protegerse contra las amenazas cibernéticas más peligrosas. Los controles se han desarrollado a partir de la experiencia de expertos en ciberseguridad de todo el mundo y se basan en las mejores prácticas del sector. Los controles están diseñados para ser implementados en tres fases, con seis controles en cada fase (Engine, 2023)**.**

Los 18 controles del CIS se dividen en tres grupos:

Proteger: Los seis primeros controles se centran en establecer los fundamentos de un programa sólido de ciberseguridad.

Detectar: Los seis controles siguientes se centran en la detección temprana de amenazas cibernéticas.

Responder: Los seis últimos controles se centran en la respuesta rápida y efectiva a las amenazas cibernéticas.

Investigaciones previas realizadas

Hay diversas investigaciones realizadas que se enfocan en mejorar la seguridad en las redes de manera general, pero no hay muchas que sean específicas para redes OT, vamos a revisar algunas de las investigaciones que se podrían relacionar con la propuesta de este plan de seguridad:

En la actualidad, es muy importante considerar que la información es una prioridad para cualquier institución u organización. Dentro de estas entidades, la información conjuntamente con los sistemas informáticos y procesos, forman activos muy importantes. La confidencialidad, disponibilidad e integridad de la información deben ser garantizadas, para mantener niveles de conformidad, competitividad e imagen empresarial (Chicaiza y Torres, 2020).

El objetivo de un sistema de gestión de seguridad de la información, es cumplir con los requerimientos de la empresa, satisfacer sus necesidades en cuanto a seguridad; y, sobre todo, integrarse con los procesos de la organización. El personal requiere concientización sobre la importancia de su rol para la gestión de la información y un sistema, que facilite su uso mediante reglas que brinden seguridad, pero no interrumpan el normal desarrollo de las actividades y funciones de la empresa (Acurio y Moya, 2023).

Cada día aparecen nuevas amenazas que ponen en riesgos los sistemas informáticos, los delincuentes actúan de muchas formas, buscando detectar vulnerabilidades para penetrar los sistemas de información y las motivaciones que los impulsan pueden ser de distinta índole, algunos lo hacen por ocio, pero la gran mayoría lo hace con fines delictivos. Frente a esto, las empresas invierten en mecanismos de protección para mitigar los riesgos mediante la implementación de firewall, antivirus, protección por medio de contraseñas, etc. Sin embargo, estas medidas pueden ser insuficientes debido a que las amenazas se mantienen una constante evolución y diversificación (Quiroga, 2021).

Francés (2022), los gobiernos se han visto obligados a desarrollar estrategias para garantizar la seguridad de sus infraestructuras críticas (CI, critical infrastructure), es decir, de las instalaciones y sistemas de servicios esenciales (p.ej.: centrales eléctricas).

Se podría entender que la protección de las infraestructuras críticas, se refiere a la ciberseguridad industrial. Sin embargo, la mayoría de las infraestructuras industriales no están catalogadas como CI y lo mismo sucede al, como es el caso del sector de la salud.

Centrándonos en lo que nos interesa para este proyecto, la OT está dedicada a detectar o cambiar los procesos físicos a través del monitoreo y administración de dispositivos. Como resultará comprensible, esta actividad está muy ligada al entorno industrial, donde se requiere de un control continuo de elementos como tuberías, válvulas o disyuntores.

A diferencia del sector IT tradicional, los entornos OT tienen un ritmo en lo referido a la seguridad informática totalmente distinto. Se trata de entornos los cuales fueron diseñados hace años para operar de forma aislada, inclusive en algunos casos en localizaciones remotas, poco accesibles o inhóspitas. Sin embargo, fruto de la incorporación de nuevas tecnologías se han sometido a una evolución de interconexión de componentes, con el objetivo de optimizar procesos que permitan mejorar la producción. Estos cambios han provocado la sobreexposición de dispositivos sin elementos y mecanismos de seguridad, de forma que se han perfilado estos entornos como muy apetecibles para posibles atacantes, además de por su gran impacto (Scatton, 2021).

1.2. Proceso investigativo metodológico

Para este proceso de investigación se usó en primer lugar la investigación bibliográfica, que consiste en la revisión de material bibliográfico existente con respecto al tema a estudiar. Esta técnica es fundamental para realizar trabajos de investigación y puede ser tan superficial o profunda como se decida. La investigación para el plan de seguridad informática en la red OT de la mina combinó dos enfoques: revisión bibliográfica y entrevista al administrador de la red. La revisión brindó información sobre vulnerabilidades, buenas prácticas y metodologías de análisis. La entrevista **ANEXO 1** permitió conocer la infraestructura, necesidades y contexto de la red, validando la información de la revisión. La combinación de ambos enfoques permitió un plan más preciso, adaptado y efectivo, con mayor compromiso del administrador. En segundo lugar, se usó la investigación descriptiva ya que su objetivo es proporcionar una representación de los hechos y características de la investigación sin manipular ninguna variable.

A través del análisis crítico, se evaluará diversas pautas relacionadas a la tecnología operativa y las recomendaciones existentes para conseguir que se pueda cumplir las normas de seguridad necesaria en la industria. Usando la observación y la experimentación se verificará si las configuraciones, sistemas y controles actuales cumplen con las condiciones de seguridad adecuadas en el entorno investigado.

Para poder recolectar la información que definirá los objetivos de este trabajo, se usaron sensores de red de Nozomi Networks para capturar la información sobre los sistemas de red y comunicaciones en el entorno OT, obteniendo de esta manera archivos de configuración que permitieron generar un informe detallado.

El lugar de la investigación fue en una mina ubicada en el sur del Ecuador, y donde se encuentra la cubierta y la planta de procesos, que es en donde están todos los dispositivos de la red OT que fueron escaneados para esta investigación. Estamos hablando de una red de alrededor de 500 dispositivos.

Se optó por usa la metodología ágil SCRUM, ya que es una forma de desarrollo de proyectos caracterizada por un seguimiento continuo, flexible y periódico del trabajo. Se basa en la colaboración, la rapidez y la efectividad, y está respaldada por datos. En la investigación científica, esta metodología ágil puede ser utilizada para la gestión de proyectos de investigación, permitiendo una mayor flexibilidad y adaptabilidad a los cambios en el proyecto, y una mayor colaboración y retroalimentación entre los miembros del equipo de investigación y las partes interesadas (Gonçalves, 2023).

1.3. Análisis de resultados

La entrevista realizada al administrador de la red OT en la mina, fue un componente crucial para el desarrollo de un plan de seguridad informática eficaz. A través de esta interacción, se logró:

Comprensión Profunda de la Red OT:

- Se obtuvo información detallada sobre la arquitectura, componentes, funciones y flujos de datos de la red OT.
- Se identificaron los activos críticos y los procesos que dependen de la red OT.
- Se comprendieron las vulnerabilidades y riesgos específicos a los que está expuesta la red.

Justificación del Plan de Seguridad:

- Se validó la necesidad urgente de implementar un plan de seguridad para proteger la red OT de las amenazas cibernéticas.
- Se confirmaron las consecuencias potenciales de un ataque a la red OT, incluyendo la pérdida de producción, daños a la infraestructura y riesgos para la seguridad del personal.

Verificación de Permisos para el Sensor de Nozomi Networks:

- Se verificaron los permisos y configuraciones necesarios para el sensor que realizó el análisis de la red OT.
- Se aseguraron las condiciones para una operación segura y confiable del sensor.

El análisis exhaustivo de la información recopilada en la red OT de la mina, ha permitido identificar una serie de riesgos y vulnerabilidades que requieren atención inmediata. La **Tabla 1** presenta un resumen detallado de estos hallazgos, junto con sus implicaciones.

Tabla 1

Riesgos y vulnerabilidades encontrados en la red OT

#	Observación	Implicación
1	**Sin visibilidad, registro ni supervisión:** No se recopilan registros de ningún sistema que no sea el firewall. No hay visibilidad del tráfico de red y no se conoce una buena línea de base.	• Será difícil detectar o responder a un ataque o incidente sin ninguna visibilidad. • No hay capacidad de revisar la información histórica para determinar lo que ha ocurrido en el pasado. • No es posible identificar amenazas o anomalías.
2	**Inventario manual de activos de hardware y software:** Aunque existe un inventario de activos, se mantiene manualmente.	• Las protecciones pueden no aplicarse a todos los activos si no se conocen todos. • La respuesta a incidentes es difícil cuando no se conocen todos los activos. • Las desviaciones de la norma son difíciles de detectar cuando no se conocen los activos".
3	**Las copias de seguridad se realizan manualmente:** Se realizan copias de seguridad de todos los sistemas, sin embargo, las copias de seguridad del firmware y la configuración de OT son manuales.	• El personal puede olvidarse de hacer copias de seguridad y puede que no se hagan después de cada cambio. • Con personal múltiple, las copias de seguridad pueden ser realizadas de forma diferente por diferentes personal. • Las copias de seguridad pueden no almacenarse de forma segura.
4	**Las copias de seguridad no son inmutables:** Las copias de seguridad se duplican en el centro de datos de recuperación, pero no hay copias offline.	• Los datos de ambos centros de datos, podrían perderse debido a errores humanos, ransomware o sucesos del mundo real.
5	**Active Directory no ha sido reforzado:** Los sistemas OT Windows se gestionan con Active Directory, sin embargo, Active Directory no ha sido reforzado.	• Active Directory, presenta una superficie de ataque muy grande que los atacantes tienen práctica en comprometer. • Si se compromete Active Directory, es probable que se comprometan TODOS los sistemas OT.
6	**La configuración de los end point de Windows no está reforzada:** Los servidores y PC de trabajo Windows no tienen una configuración de base segura.	• Si un atacante consiguiera acceder al entorno OT, sería fácil comprometer los sistemas Windows y pasar de uno a otro.

7	**La configuración de los dispositivos de red no está reforzada:** El registro no está habilitado, los puertos no utilizados y los servicios web no están deshabilitados. Algunos switches no tienen autenticación configurada.	• Los dispositivos de red controlan todos los accesos a los sistemas de OT. Un ataque a la infraestructura de red, puede poner en peligro todo el entorno OT. • Sin registro ni supervisión, no es posible detectar un ataque contra la infraestructura de red.
8	**La red OT no está completamente segregada de la red corporativa:** Se permite cierta comunicación SCADA-PCS-GR_01 directamente a CORPORATE-LPE_LIMS_01.	• Toda comunicación entre las redes de TI y OT debe pasar a través de una DMZ. Al permitir la comunicación directa, es más probable que un agente de amenazas pueda establecer una conexión completa de mando y control desde la red OT a Internet a través de la red corporativa.
9	**No existe un plan de respuesta a incidentes específico para OT:** Existe un plan corporativo de respuesta a incidentes, pero la personalización y las pruebas en OT son limitadas. No existe un retenedor de Respuesta a Incidentes (IR).	• La respuesta dependería de que el personal disponible tome las medidas adecuadas. • El apoyo externo puede ser difícil de obtener sin un anticipo o un plan establecido con los proveedores. • La contención, erradicación y recuperación pueden llevar más tiempo del previsto debido a la falta de práctica. • Pueden surgir retos inesperados durante la respuesta.
10	**Gestión de vulnerabilidades y parches limitada:** Los parches sólo se aplican por indicación del proveedor. No hay una gestión activa de las vulnerabilidades.	• Si un atacante obtuviera acceso a cualquier sistema OT, probablemente podría elevar privilegios y obtener un acceso significativo al entorno. • La organización no es consciente de su exposición actual al riesgo debido a la falta de información.
11	**Las mejores prácticas de configuración de la infraestructura de red se aplican de forma incoherente:** La VLAN 1 está en uso, no hay protecciones habilitadas contra ataques machine-in-the-middle y otros.	• Varios ataques son más fáciles de ejecutar cuando se utiliza la VLAN 1. • Los ataques a nivel de red (por ejemplo, machine-in-the-middle) son más fáciles de llevar a cabo cuando las protecciones no están activadas.
12	**La gestión de las infraestructuras corre a cargo de los técnicos de instrumentación y control:** Los técnicos no tienen formación en infraestructuras y no disponen del tiempo necesario para gestionar toda la infraestructura.	• Sin formación y experiencia especializadas, los técnicos no tendrán los conocimientos profundos y la experiencia necesarios para proteger adecuadamente las redes y la infraestructura. • Incluso cuando tengan conocimientos, sin tiempo para dedicar a la gestión de la infraestructura, muchas tareas básicas de configuración y seguridad no se completarán.

13	**Se depende de los conocimientos no documentados que poseen los recursos clave:** Se confía mucho en los conocimientos del Administrador OT sobre el entorno que no están formalmente documentados.	• Si el Administrador OT dejara la organización o no estuviera disponible por cualquier otro motivo, se perdería una gran cantidad de conocimientos. • Podría resultar difícil recuperar o actualizar algunos sistemas y dispositivos si el Administrador OT no está disponible.
14	**Las políticas de contraseñas no están definidas ni se aplican:** No hay una política de contraseñas definida para los dispositivos OT. Las contraseñas locales se utilizan en muchos sistemas como la infraestructura de red y los PLC.	• Los usuarios pueden elegir contraseñas débiles que pueden ser adivinadas por un atacante. • Los usuarios que abandonan la organización pueden conservar las contraseñas de acceso. • No es posible rastrear o correlacionar acciones a un individuo cuando las cuentas son compartidas.
15	**No hay gestión centralizada de los equipos OT:** La configuración de los controladores se gestiona dispositivo por dispositivo. Las actualizaciones de firmware se aplican manualmente.	• Los dispositivos pueden ejecutar software no actualizado. • Es difícil detectar cambios malintencionados en la configuración o el firmware. • Es más difícil mantener una versión de software y una configuración. • La exposición a los ataques aumenta cuando hay varias versiones diferentes y desactualizadas de software o firmware en uso.
16	**Los switches de la planta de pasta son físicamente inseguros y carecen de autenticación de inicio de sesión:** No se requiere autenticación para acceder a los conmutadores, la sala donde se encuentran no está cerrada con llave y su bastidor está separado de la pared.	• Puede producirse un apagón si el rack se cae o si los dispositivos fallan debido a las vibraciones, el polvo o la suciedad. • Cualquiera con acceso físico a la planta podría acceder a la infraestructura de red a través de la cual podría acceder a todos los sistemas de la red.
17	**Se ha descubierto un switch desconocido y no gestionado:** Su propósito no está claro y la personal in situ no puede acceder al switch.	• El personal no dispone de un inventario completo. • Si el interruptor fallara, podría ser difícil sustituirlo con precisión. • El interruptor no está siendo actualizado y por lo tanto podría estar sujeto a vulnerabilidades
18	**No se utiliza la tecnología de contraseñas seguras:** En muchos dispositivos se utilizan contraseñas locales. Estas contraseñas no se almacenan de forma segura en una ubicación central	• Las contraseñas elegidas pueden ser más débiles de lo óptimo si hay que recordarlas. • No hay forma segura de compartir contraseñas entre usuarios. • Las contraseñas serán conocidas por los usuarios, mientras que algunas cajas fuertes de contraseñas pueden iniciar sesión sin revelar las contraseñas. • No hay forma de que otros determinen las contraseñas si el personal con conocimiento de las contraseñas no está disponible.

19	**Los protocolos innecesarios están habilitados:** Protocolos como IPv6 que un atacante podría aprovechar en un ataque están habilitados.	•Los atacantes pueden aprovecharse de estos protocolos para interceptar y modificar la comunicación y controlar la vista de red de los dispositivos.
20	**Segregación limitada dentro de la red OT:** Aunque la red de procesos está separada de la red SCADA, hay muchos servidores ulti-homed que sirven de puente entre ambas. No hay segmentación dentro de la red SCADA, donde se conectan sistemas con muchos propósitos diferentes.	• Aunque las redes están separadas, el compromiso de un solo servidor podría permitir a un atacante atravesar las redes. • Con acceso a un único sistema de la red SCADA, un atacante puede interactuar con todos los demás sistemas SCADA y, a través de ellos, con la red de control de procesos.
21	**Vulnerabilidades conocidas:** Se detectaron vulnerabilidades conocidas en switches y routers Cisco, así como en algunos PLC de Schneider.	• Existen exploits que podrían utilizarse para tomar el control de la infraestructura de red si un atacante puede acceder a la red. • Pueden existir otros fallos operativos que podrían causar una interrupción.

CAPÍTULO II: PROPUESTA

2.1 Fundamentos teóricos aplicados

La elaboración de este plan de seguridad informática se basa en el cumplimiento de los 18 controles del CIS, ya que estos son un conjunto de acciones desarrolladas por una comunidad de TI globalizada, que se basan en las mejores prácticas usadas por diversas empresas a nivel mundial para protegerse de las amenazas cibernéticas más comunes (Centro para la Seguridad de Internet, 2024).

Según el documento (Center for Internet Security, 2021), estos consisten en 18 controles que se pueden implementar de forma independiente o como parte de un programa de seguridad integral.

Los Controles del CIS se basan en los siguientes principios:

Defensa en profundidad: Implementar múltiples capas de seguridad para proteger los activos de la organización.

Principio de menor privilegio: Otorgar a los usuarios solo el acceso que necesitan para realizar sus trabajos.

Seguridad por defecto: Configurar los sistemas y dispositivos de forma segura por defecto.

Concienciación y formación en seguridad: Educar a los empleados sobre las amenazas cibernéticas y cómo protegerse a sí mismos y a la organización.

Monitoreo y revisión continua: Monitorizar y revisar el plan de seguridad de forma continua para asegurar que sigue siendo eficaz.

Los Controles CIS son reconocidos como una de las mejores prácticas para la seguridad informática por las siguientes razones:

Están basados en evidencia: Se basan en el análisis de las amenazas cibernéticas más comunes y en las mejores prácticas para mitigarlas.

Son flexibles: Se pueden adaptar a las necesidades específicas de cualquier organización.

Son rentables: Se pueden implementar de forma gradual y económica.

Son ampliamente aceptados: Son utilizados por organizaciones de todo el mundo.

Los Controles CIS son una herramienta valiosa para cualquier organización que quiera mejorar su postura de seguridad informática.

A continuación, se presenta una lista de los 18 Controles del CIS:

1. **Inventario y control de activos:** Identificar y controlar todos los activos de hardware, software y datos de la organización.
2. **Gestión de vulnerabilidades:** Identificar y corregir las vulnerabilidades de seguridad de forma oportuna.
3. **Credenciales seguras:** Implementar medidas de seguridad para las credenciales de usuario, como contraseñas y tokens.

4. **Control de acceso:** Limitar el acceso a los recursos de la organización a los usuarios autorizados.
5. **Datos seguros:** Proteger la confidencialidad, integridad y disponibilidad de los datos.
6. **Seguridad de software:** Implementar medidas de seguridad para el software, como el control de versiones y la gestión de parches.
7. **Comunicaciones seguras:** Proteger las comunicaciones de la organización contra la interceptación, la modificación y la falsificación.
8. **Concienciación y formación en seguridad:** Educar a los empleados sobre las amenazas cibernéticas y cómo protegerse a sí mismos y a la organización.
9. **Gestión de dispositivos:** Implementar medidas de seguridad para los dispositivos, como el control de acceso y el cifrado.
10. **Seguridad de la infraestructura de red:** Proteger la infraestructura de red de la organización contra ataques.
11. **Supervisión y registro de la seguridad:** Monitorizar y registrar la actividad de seguridad de la organización.
12. **Respuesta a incidentes:** Implementar un plan de respuesta a incidentes para responder a las amenazas cibernéticas.
13. **Recuperación ante desastres:** Implementar un plan de recuperación ante desastres para restaurar la capacidad de la organización en caso de un desastre.
14. **Gestión de proveedores de servicios:** Implementar medidas de seguridad para los proveedores de servicios de la organización.
15. **Gestión de aplicaciones:** Implementar medidas de seguridad para las aplicaciones de la organización.
16. **Gestión de la seguridad en la nube:** Implementar medidas de seguridad para los recursos en la nube de la organización.
17. **Inteligencia de amenazas:** Obtener información sobre las amenazas cibernéticas para mejorar la postura de seguridad de la organización.
18. **Mejora continua de la seguridad:** Implementar un proceso de mejora continua para el programa de seguridad de la organización.

Los Cinco Controles Críticos de Ciberseguridad para ICS / OT

Los Cinco Controles Críticos de Ciberseguridad para ICS / OT (**Figura 2**), son un subconjunto conciso de prácticas de seguridad esenciales desarrolladas específicamente para sistemas de control industrial

(ICS) y entornos de tecnología operativa (OT). Su objetivo es abordar las vulnerabilidades y riesgos únicos presentes en estos sistemas de infraestructura crítica (SANS, 2022).

Figura 2

Los cinco controles de ciberseguridad para ICS / OT

Estos cinco controles priorizan las acciones más críticas para mitigar proactivamente:

- Acceso no autorizado
- Pérdida de control
- Violaciones de datos
- Interrupciones en las operaciones

Si bien marcos más amplios como CIS Controls 18, ofrecen una guía completa, Los Cinco Controles Críticos de Ciberseguridad para ICS / OT proporcionan un enfoque centrado y práctico para las necesidades específicas de OT. A continuación, en base al documento (M. Lee y Conway, 2022) se presenta el detalle de estos cinco controles críticos:

1. **Respuesta a incidentes de Sistemas de control Industrial:** Los planes de respuesta a incidentes basados en operaciones, se centran en la integridad y la resiliencia del sistema y están diseñados para reducir la complejidad de responder a los ataques en el entorno operativo. Estos ejercicios refuerzan los escenarios de riesgo y de usuario adaptados a su entorno de seguridad, priorizando acciones en función del impacto potencial de una acción y cómo posicionar los sistemas para responder a los ataques. También mejoran la resiliencia operativa al facilitar el análisis de la causa raíz de fallas potenciales.
2. **Arquitectura Defendible:** Una arquitectura defendible ICS eficaz admite procesos de visibilidad,

registro, identificación de activos, segmentación, DMZ industrial y comunicación compatible. Ayuda a cerrar la brecha entre la tecnología y las personas al reducir el riesgo a través del diseño y la implementación del sistema mientras impulsa procesos efectivos del equipo de seguridad.

3. **Supervisión de la visibilidad de la red ICS:** Debido a la naturaleza de "sistemas de sistemas" de los ataques a ICS, es fundamental el monitoreo continuo de la ciberseguridad del entorno de ICS mediante kits de herramientas compatibles con el protocolo y el análisis de las interacciones entre sistemas. Estas capacidades se pueden utilizar para informar a los equipos de operaciones sobre posibles vulnerabilidades que deben abordarse, lo que ayuda a garantizar la resiliencia y la recuperación general.
4. **Seguridad de acceso remoto:** A medida que la sociedad adopta un marco híbrido basado en la nube, los atacantes aprovechan cada vez más el acceso remoto para penetrar las redes OT. En el pasado, la forma principal de atacar una red OT era a través de la red de TI de la organización, pero ahora los actores de amenazas también pueden explotar las vulnerabilidades de la red de TI en toda la cadena de suministro. A su vez, mantener un control de acceso remoto seguro no es negociable para las operaciones industriales actuales.
5. **Gestión de vulnerabilidades basada en riesgos:** Un programa de gestión de vulnerabilidades basado en riesgos, permite a las organizaciones definir y priorizar las vulnerabilidades de ICS que plantean el mayor nivel de riesgo. Estas vulnerabilidades, a menudo brindan a los atacantes acceso a ICS o introducen nuevas funciones que pueden usarse para crear problemas operativos como pérdida de visibilidad, control o seguridad en un entorno industrial. La adopción de una gestión de la vulnerabilidad basada en el riesgo, requiere control y condiciones operativas del equipo para facilitar la toma de decisiones basada en el riesgo durante las actividades de prevención, respuesta, remediación y recuperación.

Beneficios de Implementar Los Cinco Controles Críticos de Ciberseguridad para ICS:

Reducir los riesgos de ciberseguridad: al abordar las vulnerabilidades más críticas, las organizaciones pueden reducir importantes riesgos de seguridad en sus entornos ICS.

Estabilidad operativa mejorada: la seguridad mejorada ayuda a prevenir interrupciones y garantiza el funcionamiento confiable de la infraestructura crítica.

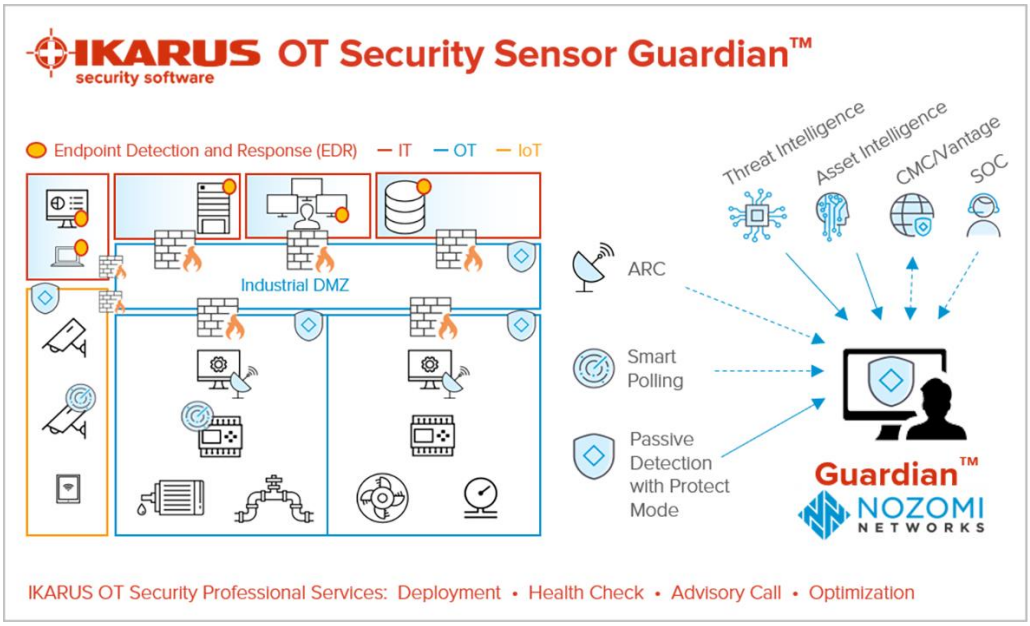
Cumplimiento normativo: muchas regulaciones y estándares de la industria, requieren la implementación de estos controles para demostrar los esfuerzos de cumplimiento.

Además de los Controles CIS, se usaron sensores de Nozomi Networks **Figura 3**, esta empresa es líder en ciberseguridad OT e iOT, que ofrece soluciones de seguridad y visibilidad para entornos

industriales. Fundada en 2013 y con sede en San Francisco, California, Nozomi Networks proporciona visibilidad en tiempo real de todos los activos y redes, identificando y supervisando cada dispositivo IoT, OT e ICS de los entornos operativos, incluyendo funciones, protocolos, flujos de datos y mucho más. La plataforma de Nozomi Networks combina el descubrimiento de activos, visualización de redes, evaluación de vulnerabilidades, monitoreo de riesgos y detección de amenazas cibernéticas en una sola plataforma. Los clientes de Nozomi Networks, incluyen sectores de infraestructura crítica como energía, fabricación y salud, y la empresa sirve a clientes en todo el mundo. Nozomi Networks, también ofrece soluciones de gestión de seguridad in situ y un motor de análisis y respuesta basado en IA llamado Vantage IQ (Nozomi Networks, 2024).

Figura 3

Ejemplo de funcionamiento de sensor Nozomi Networks



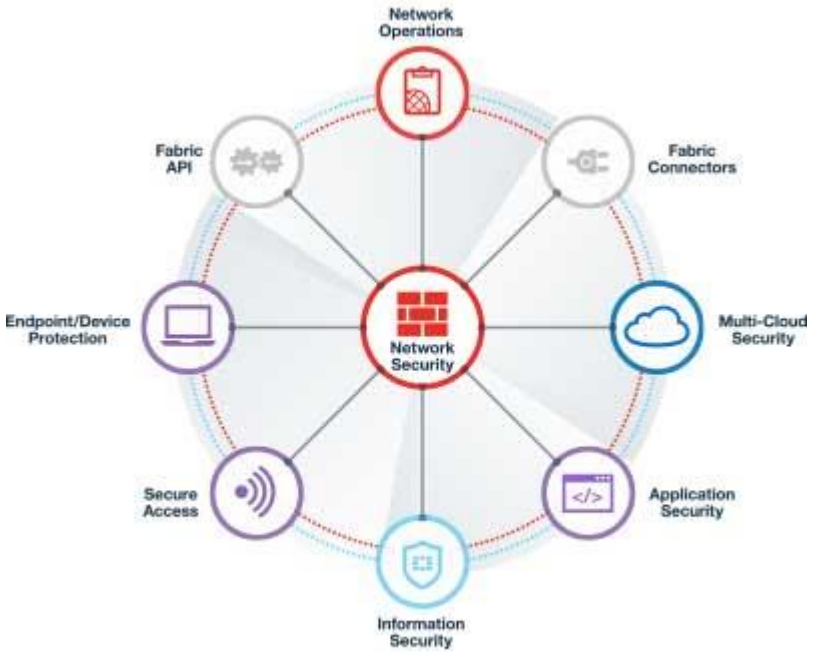
Red de Tecnología Operativa

Una red OT (**Figura 4**) es una red de Tecnología Operativa, que se utiliza para controlar y monitorear procesos físicos en entornos industriales. La OT se utiliza para interactuar con el mundo físico y se contrapone con la Tecnología de la Información (TI), la cual se ocupa de los sistemas de datos y se utiliza principalmente para resolver problemas empresariales. Las redes OT están expuestas a ataques y amenazas de diversos tipos, como malware, hackers, error humano y spear phishing, entre otros. Es

importante contar con expertos en ciberseguridad para prevenir ataques y responder de forma rápida ante cualquier tipo de amenaza (Pirosanto, 2019).

Figura 4

Esquema de una red OT



Las redes OT son el próximo gran objetivo de los ciberataques a empresas, por lo que es importante implementar soluciones de ciberseguridad que protejan mejor a los sistemas OT y que sean capaces de cumplir con las demandas más exigentes de seguridad, desempeño y abordaje (Canvia, 2023).

Las principales amenazas cibernéticas que afectan a las redes OT incluyen:

1. **Malware:** Programas maliciosos como virus, spyware y otros que pueden afectar la disponibilidad de la red y los sistemas clave.
2. **Hackers:** Personas o grupos con intenciones maliciosas que intentan obtener acceso a los componentes clave de las redes SCADA.
3. **Error humano:** Errores cometidos por los trabajadores, que pueden ser intencionales o debido a una mala capacitación o mal uso de las herramientas.
4. **Spear phishing:** Fraudes que se utilizan para obtener información personal, como usuarios, contraseñas, pero no de forma genérica como el phishing tradicional.
5. **Vulnerabilidades en los controladores industriales:** La mayoría de los controladores industriales más utilizados presentan vulnerabilidades sin parches de seguridad.

Estas amenazas pueden llevar a incidentes de seguridad en las redes OT, lo que puede poner en riesgo la disponibilidad, integridad y confidencialidad de los sistemas y procesos industriales (Canvia, 2023).

SCADA

SCADA (Supervisión y Control de Automatización Distribuida) es un sistema de automatización que permite la supervisión y control de procesos industriales y de infraestructura crítica. SCADA se utiliza en entornos como la industria petrolera, el suministro de agua y energía, y la fabricación. Este sistema permite la comunicación entre los sistemas de control y los dispositivos de campo, como sensores y actuadores, y proporciona una interfaz de usuario que permite a los operadores visualizar y controlar los procesos en tiempo real como se muestra en la **Figura 5**. SCADA es fundamental para la seguridad de las redes OT y es un objetivo común de los ciberataques.

Figura 5

Ejemplo de Supervisión SCADA

Las redes OT, a su vez, engloban todas las tecnologías destinadas a salvaguardar la información, activos y personas, y se utilizan para controlar y supervisar los dispositivos físicos, así como los procesos y eventos en entornos industriales. El SCADA es fundamental para la seguridad de las redes OT y es un objetivo común de los ciberataques (Pirosanto, 2019).

2.2 Descripción de la propuesta

La automatización de los procesos industriales abre enormes oportunidades, algunas de las cuales pueden ser muy necesarias para la humanidad. Dadas las oportunidades que enfrentan las tecnologías existentes como la nube, big data, aprendizaje automático, inteligencia artificial, IoT, 5G, etc., estas tecnologías también enfrentan amenazas. Hasta hace poco, existía una falsa sensación de seguridad en los entornos industriales basada en la creencia de que los riesgos no existían. Este sentimiento se basa principalmente en cinco ideas preconcebidas:

- La red OT está aislada y no conectada a Internet.
- Tenemos cortafuegos para protegernos.
- Los piratas informáticos no comprenden los sistemas/procesos industriales.
- Mi mina no es el objetivo de nadie.
- Los sistemas de seguridad de las fábricas o minas nos protegen de los ciberataques.

Los riesgos que hay que gestionar, se relacionan con la posibilidad de que los activos no puedan brindar servicios o pierdan su integridad para brindar servicios o sufran daños (impacto).

En los últimos años, la visibilidad o presencia de las redes OT en el entorno industrial ha aumentado, por lo que, aumenta la probabilidad de que se produzca un incidente de seguridad cibernética. Actualmente, los sistemas OT sufren los mismos problemas heredados que los sistemas TI (Tecnologías de la Información) debido a la consolidación y conectividad que estamos experimentando.

El entorno OT de la mina está casi completamente aislado de la red corporativa y no tiene conexión a internet. Esto reduce significativamente la superficie de ataque expuesta a actores maliciosos, limitando la probabilidad de un ataque exitoso. Adicionalmente no se permite el acceso remoto a la red OT excepto desde sistemas corporativos seleccionados. Esto proporciona a la mina una postura de seguridad muy sólida y compensa algunos de los problemas identificados en la red OT.

Se cree que, con el tiempo, es probable que se requiera cada vez más conectividad entre las redes OT, IT e Internet. Observamos una demanda creciente de transferencia de datos entre redes IT y OT, así como acceso remoto de proveedores y personal desde Internet y conectividad con proveedores y otros terceros.

En consecuencia, se piensa que será cada vez más difícil para la mina mantener el aislamiento actual de la red. A medida que el aislamiento se reduzca gradualmente, el riesgo debido a los hallazgos encontrados aumentará a medida que se expongan a más personas, sistemas y redes. Vamos a procurar mitigar todos los riesgos y vulnerabilidades encontrados en la red OT de la empresa minera usando los conceptos y buenas prácticas establecidos en los fundamentos teóricos del presente documento.

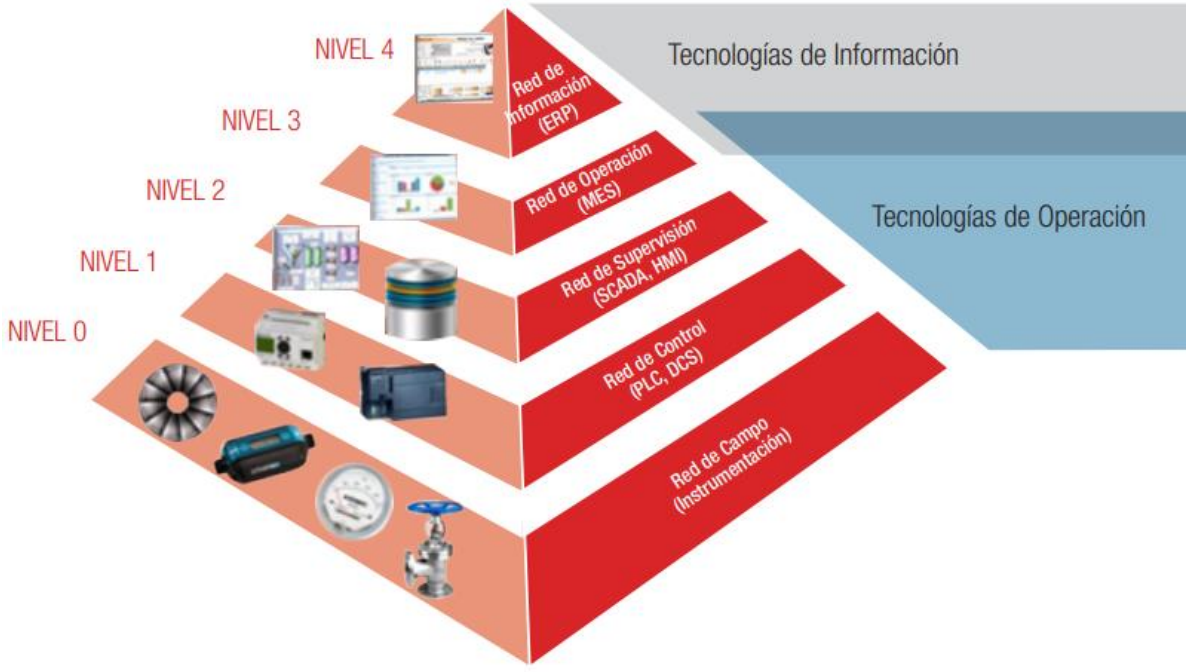
2.2.1 Estructura general

Las tecnologías destinadas a la automatización y el control de los procesos productivos se organizan en lo que se denomina "pirámide de automatización". Este modelo conceptual representa cómo se distribuyen y relacionan las diferentes capas de tecnología dentro de un entorno industrial, abarcando desde la recolección de datos en el campo hasta la toma de decisiones estratégicas a nivel empresarial. La pirámide es un reflejo de la jerarquía tecnológica que facilita la integración y la comunicación eficaz entre los diversos componentes y sistemas operativos.

Cada nivel de la pirámide tiene un papel crucial en el aseguramiento de que los procesos industriales sean más eficientes, seguros y flexibles. La automatización no solo mejora la precisión y la velocidad de la producción, sino que también contribuye a la reducción de costos y al aumento de la calidad del producto final. Además, permite una mejor gestión de los recursos y una respuesta más rápida ante las demandas cambiantes del mercado, se muestra un esquema en la **Figura 6**.

Figura 6

Pirámide de Automatización



Actualmente la estructura de red de la mina se divide en estos 5 niveles:

Nivel 0.- Nivel de datos de campo o recopilación de instrumentos, es decir, Los sensores y actuadores están distribuidos por todo el proceso y permiten el control de las máquinas y equipos de producción. En este nivel se encuentran todos los sensores y procesos relacionados a la extracción de minerales de la mina.

Nivel 1.- Nivel donde se agrupan todos los controladores locales, por ejemplo: PC, PLC, etc. Las máquinas de este nivel utilizarán datos de proceso de instrumentos de NIVEL 0 y emitirán comandos a los actuadores.

Nivel 2.- En este nivel se encuentra el grado de supervisión de los equipos diseñados para controlar la secuencia de trituración, extracción, etc. Por ejemplo: SCADA, estación de operador o servidor de ingeniería.

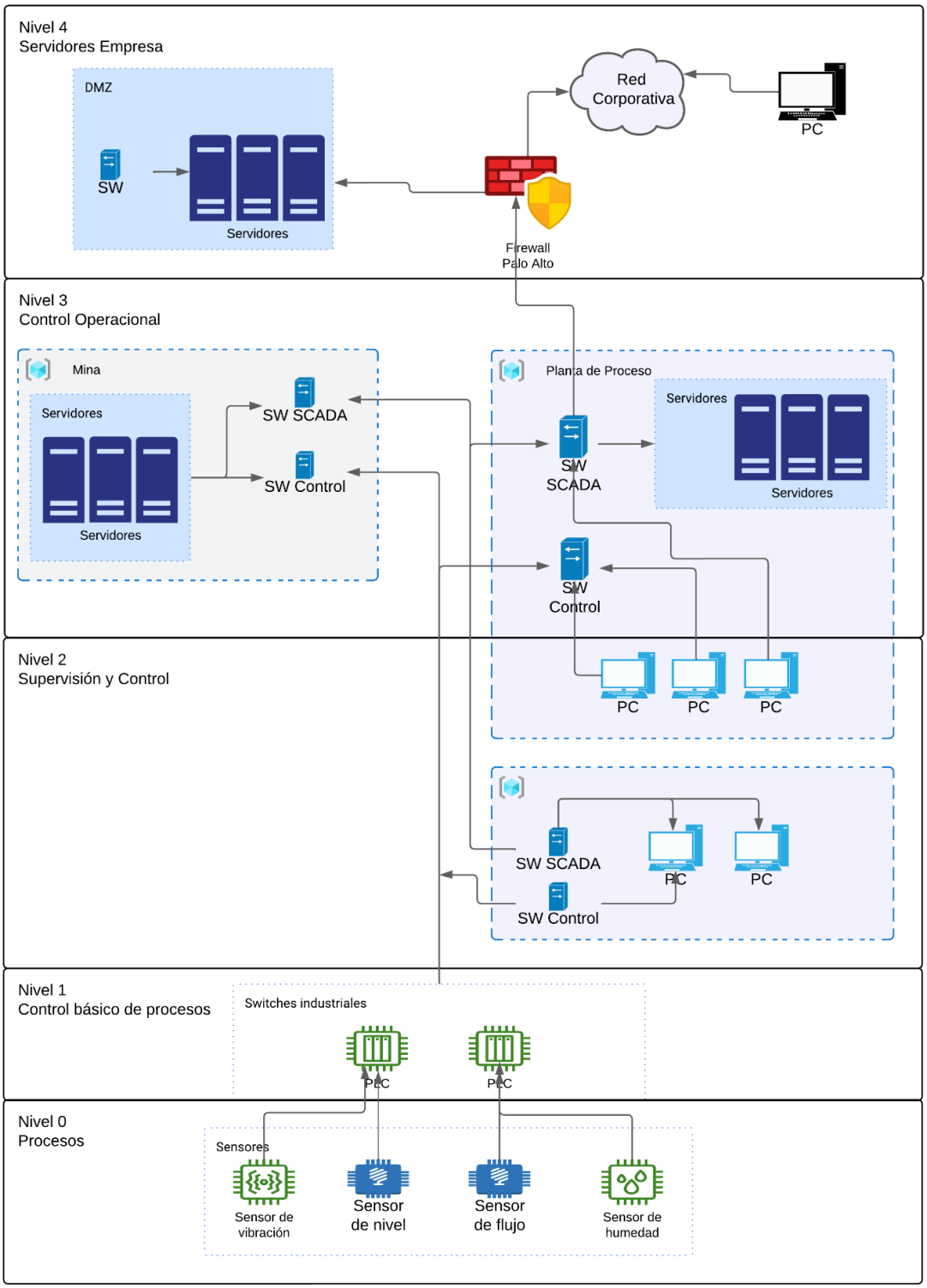
Nivel 3.- El nivel de actividad de producción controla el flujo de trabajo para producir u optimizar el producto final, en este nivel ya encontramos a los equipos y servidores encargados del control de toda la operación en la mina y en la planta de proceso.

Nivel 4.- El nivel de gestión donde se desarrollan todas las actividades necesarias relacionadas con el negocio de la organización industrial y se mantiene la comunicación con proveedores y clientes. En este nivel tenemos la zona desmilitarizada Industrial con los servidores de la empresa como tal y la conexión a la red corporativa (TI) a través de un Firewall Palo Alto.

En la **Figura *7*** se muestra de manera gráfica la estructura de la red OT en general.

Figura 7

Arquitectura de la red OT de la mina



2.2.2 Explicación del aporte

Las redes OT en una mina, desempeñan un papel fundamental en el control y monitoreo de los procesos físicos esenciales para la operación minera. Estas redes son cruciales para la gestión eficiente de la maquinaria, los sistemas de transporte, la vigilancia de las condiciones ambientales, y la garantía de la seguridad de los trabajadores. Su implementación asegura una operación minera más segura, eficaz y optimizada.

Un plan de seguridad informática en redes OT es crucial por las siguientes razones:

1. Impacto en la seguridad y el bienestar de los trabajadores:

Un ataque cibernético a la red OT podría provocar fallos en los sistemas de control, poniendo en riesgo la seguridad de los trabajadores y el entorno de la mina.

Los fallos en los sistemas de seguridad, como los sistemas de detección de gases o de incendios, podrían tener graves consecuencias para la salud de los trabajadores.

2. Pérdidas económicas:

La interrupción de la producción debido a un ataque cibernético o un fallo del sistema, puede ocasionar importantes pérdidas económicas.

El robo de datos sensibles, como información geológica o financiera, puede tener un impacto negativo en la competitividad de la empresa.

3. Daños a la reputación:

Un incidente de seguridad informática puede dañar la reputación de la empresa minera y afectar la confianza de sus clientes, proveedores e inversores.

4. Cumplimiento normativo:

Las empresas mineras están sujetas a diversas normas y regulaciones que exigen la implementación de medidas de seguridad informática para proteger sus sistemas y datos.

A continuación, se presentan algunos ejemplos específicos de riesgos de seguridad en redes OT en una mina:

Ataques a los sistemas de control: Los atacantes pueden tomar el control de los sistemas de control para causar daños físicos a la infraestructura o manipular los procesos de producción.

Malware: Los programas maliciosos pueden infectar los sistemas OT y causar daños a los equipos, la pérdida de datos o la interrupción de los procesos.

Acceso no autorizado: Los actores malintencionados pueden obtener acceso no autorizado a la red OT para robar datos sensibles o espiar las operaciones de la mina.

Fallos de seguridad: Los errores de configuración, la falta de actualizaciones de software o las prácticas de seguridad inadecuadas pueden dejar la red OT vulnerable a ataques.

Para proteger las redes OT en una mina o cualquier entorno industrial, es fundamental implementar una serie de medidas de seguridad, como:

Segmentar la red OT: Separar la red OT de la red corporativa y de internet para limitar la superficie de ataque.

Controlar el acceso: Implementar medidas de control de acceso para restringir el acceso a la red OT a usuarios autorizados.

Utilizar firewalls y sistemas de detección de intrusiones: Proteger la red OT de intrusiones no autorizadas.

Mantener el software actualizado: Aplicar parches de seguridad y actualizaciones de software para corregir vulnerabilidades conocidas.

Capacitar al personal: Concienciar al personal sobre la importancia de la seguridad informática y las mejores prácticas para proteger la red OT.

2.2.3 Estrategias y/o técnicas

Para el desarrollo del presente plan, hubo la necesidad de utilizar técnicas y estrategias:

Recopilación de información:

Análisis documental: Revisar documentos relevantes como manuales de operación, políticas de seguridad, informes de auditoría y evaluaciones de riesgos existentes.

Entrevistas: Entrevistar a personal clave de la mina, incluyendo ingenieros de OT, personal de seguridad informática, gerentes de operaciones y responsables de la toma de decisiones.

Observación directa: Visitar la mina y observar las operaciones de la red OT para comprender mejor los riesgos y las necesidades de seguridad.

Análisis de riesgos:

Identificar activos: Identificar los activos críticos de la red OT, como equipos de control, sistemas de monitorización, servidores y bases de datos.

Identificar amenazas y vulnerabilidades: Identificar las amenazas y vulnerabilidades relevantes para la red OT, como ataques cibernéticos, errores humanos, fallos de hardware y software, y desastres naturales.

Evaluar riesgos: Evaluar el impacto y la probabilidad de cada riesgo para determinar su prioridad.

Desarrollo de estrategias:

Selección de controles de seguridad: Seleccionar los controles de seguridad adecuados para mitigar los riesgos identificados, como firewalls, sistemas de detección de intrusiones, control de acceso, segmentación de red y copias de seguridad.

Diseño de la arquitectura de seguridad: Diseñar una arquitectura de seguridad robusta que integre los controles de seguridad seleccionados.

Sugerir el desarrollo de políticas y procedimientos: Desarrollar políticas y procedimientos para la gestión de la seguridad informática en la red OT, incluyendo respuesta a incidentes, gestión de parches y formación del personal.

Evaluación y validación:

Simulaciones y pruebas: Realizar simulaciones y pruebas de penetración para evaluar la eficacia de la arquitectura de seguridad y los controles implementados.

Análisis de costes y beneficios: Evaluar los costes y beneficios de la implementación del plan de seguridad informática.

Técnicas de investigación específicas:

Análisis de brechas de seguridad: Comparar la situación actual de la seguridad informática con las mejores prácticas de la industria.

Benchmarking: Comparar el plan de seguridad informática con planes de otras empresas mineras.

Análisis del entorno de amenazas: Investigar las últimas tendencias en amenazas cibernéticas para identificar las más relevantes para la red OT.

Análisis de riesgos específicos de la industria minera: Investigar los riesgos de seguridad específicos de la industria minera, como los ataques a sistemas de control industrial.

2.3 Validación de la propuesta

La validación de la propuesta del plan de seguridad informático se llevó a cabo mediante un proceso de revisión por parte de tres especialistas calificados en el ámbito de la tecnología Operativa y la seguridad informática. Estos expertos, cuya experiencia y conocimientos profundos en sus respectivos campos, evaluaron la propuesta basándose en los criterios definidos en la **Tabla 2**, este proceso de validación aseguró que la propuesta no solo fuera teóricamente sólida sino también práctica y aplicable en el entorno real de una red OT, proporcionando una base firma para su implementación, si fuera el caso.

En el **ANEXO 3** se encuentran las matrices de validación (formato de la misma en el **ANEXO 2**) revisadas por los 3 especialistas, pero hablando un poco de ellos, el primer especialista es Luis Castro, trabaja actualmente en la empresa Tecniequipos, Ingeniero en Sistemas relacionado a la industria de hidrocarburos y sistemas industriales, también tiene un Magíster en Gestión de la Industria de Hidrocarburos , adicionalmente es especialista en Gestión de Proyectos, tiene alrededor de 17 años de experiencia en mantenimientos, integraciones e implementaciones de proyectos industriales de todo tipo. El segundo especialista es David Cerón, Ingeniero en Electrónica y Redes de Información, tiene 2 maestrías, una en Gestión de la Seguridad de la información y otra en Ciberseguridad, tiene 6 años de experiencia en los campos de administración y mantenimiento de redes informáticas, adicionalmente participo en la implementación de la red OT de una de las plantas de la empresa donde trabaja actualmente. El tercer especialista es José Gallegos, Ingeniero en Informática y Ciencias de la Computación, tiene una maestría en Gerencia de Sistemas y Tecnologías de la Información, lleva más de 15 años laborando como jefe nacional de infraestructura en la empresa donde labora actualmente y ha llevado bajo su cargo varios proyectos relacionados a seguridad informática que han implementados de manera exitosa.

Tabla 2

Criterios de validación

Criterio	Descripción	Ponderación	Evidencia	Resultado
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable/No aceptable
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable/No aceptable
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable/No aceptable
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable/No aceptable

2.3.1 Resultados del análisis

Los tres especialistas evaluaron el plan de seguridad informática en un formato definido por mí persona, y de forma unánime dieron como aceptable cada uno de los criterios propuestos para evaluar tal como se muestra en la **Tabla 3**.

Tabla 3

Resultados del análisis

Criterio	Descripción	Ponderación	Calificación por especialista		
			Mg. Luis Castro	**Mg. José Gallegos**	**Mg. David Cerón**
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Aceptable	Aceptable	Aceptable
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Aceptable	Aceptable	Aceptable
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Aceptable	Aceptable	Aceptable
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Aceptable	Aceptable	Aceptable

Adicionalmente, hicieron las siguientes observaciones:

“El documento está correctamente alineado con los hallazgos en el documento de evaluación del sitio.” (Castro, 2024)

“Comparto la valoración de la matriz del plan de seguridad Informática del documento enviado. He considerado los lineamientos en la vertical de la industria, por lo cual no tengo ninguna observación.” (Cerón, 2024)

2.4 Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 4

Matriz de articulación

Ejes o partes principales del proyecto		Sustento teórico	Sustento metodológico	Estrategias/técnicas	Descripción de resultados	Instrumentos aplicados
1	**Tecnología Operativa**	Es el uso de hardware y software para monitorear y controlar los procesos físicos, los dispositivos y la infraestructura en entornos industriales o comerciales (Fortinet, 2023).	Los métodos de investigación son bibliográficos y permiten el desarrollo de conceptos detallados.	Se realizó una investigación bibliográfica acerca del funcionamiento de una red de tecnología operativa.	Entender el funcionamiento de una red OT, permite identificar de mejor manera los posibles riesgos que puede presentar ese entorno.	Fuente bibliográfica.
2	**Centro para la Seguridad de Internet**	Es una organización sin fines de lucro enfocada en crear y promover mejores prácticas de ciberseguridad (Centro para la Seguridad de Internet, 2024).	Los métodos de investigación son bibliográficos y permiten el desarrollo de conceptos detallados.	Se realizó una investigación documental acerca del CIS.	Usar buenas prácticas adoptadas a nivel mundial, minimiza la complejidad de la creación de un plan de seguridad efectivo.	Fuente bibliográfica.

3	**Controles de Seguridad Crítica de CIS**	Son un conjunto priorizado de acciones, que sirven como guías para mitigar los ataques cibernéticos más comunes (Centro para la Seguridad de Internet, 2024).	Los métodos de investigación son bibliográficos y permiten el desarrollo de conceptos detallados.	Revisión del documento CIS Controls en su versión 8.	Usar buenas prácticas adoptadas a nivel mundial, minimiza la complejidad de la creación de un plan de seguridad efectivo.	Fuente bibliográfica.
4	**Los Cinco Controles Críticos de Ciberseguridad para ICS / OT**	Son un subconjunto conciso de prácticas de seguridad esenciales desarrolladas específicamente para sistemas de control industrial (ICS) y entornos de tecnología operativa (OT) (M. Lee y Conway, 2022) .	Los métodos de investigación son bibliográficos y permiten el desarrollo de conceptos detallados.	Revisión del documento The Five ICS Cybersecurity Critical Controls del Instituto SANS.	Es importante usar prácticas específicas, que se basen en el tipo de redes que se están analizando, ya que no es lo mismo la seguridad en una red IT que una red OT.	Fuente bibliográfica.
5	**Pirámide de automatización**	Es un modelo esencial en el campo de la automatización industrial, permite explicar cómo se integran todas las tecnologías involucradas en la industria (Tutomaniac, 2023).	Los métodos de investigación son bibliográficos y permiten el desarrollo de conceptos detallados.	Se realizó una investigación bibliográfica acerca de los niveles de la pirámide de automatización.	Comprender en que niveles existen en las empresas industriales, mejora la manera en la que se aplican los controles de seguridad para los dispositivos que se tienen en el inventario y permite enfocarse en los procesos críticos de la operación	Fuente bibliográfica.

6	**Plan de seguridad informática**	Es una estrategia que determina las acciones digitales para proteger el flujo de datos recabados mediante plataformas, aplicaciones o software especializado.	Los métodos de investigación son bibliográficos y permiten el desarrollo de conceptos detallados.	A través del análisis de contenido, identificar las vulnerabilidades y riesgos en la red. A través de la entrevista, entender la necesidad del cliente para entender la problemática.	La importancia de un plan de seguridad informática radica en que si no se lo tiene, se estará expuesto a numerosos riesgos, como la fuga de información y en algunos casos responsabilidades legales.	Fuente bibliográfica.

2.5 Análisis de resultados

La **Tabla 5** proporciona un análisis detallado de los resultados obtenidos, ofreciendo un resumen exhaustivo de las vulnerabilidades identificadas en la red OT. Además, clasifica estas vulnerabilidades de acuerdo con su tipo, para una comprensión más clara de las áreas que requieren atención prioritaria.

Tabla 5

Clasificación de Riesgos y vulnerabilidades

Riesgos y vulnerabilidades generales	Detalle
Falta de Visibilidad y Control	No hay registros ni supervisión de la mayoría de los sistemas. No se conoce la línea de base del tráfico de red. Los inventarios de activos son manuales.

	Las copias de seguridad no son inmutables.
Configuraciones Inseguras	Active Directory no está reforzado. Los endpoints de Windows, los dispositivos de red y los PLC no tienen configuraciones seguras. La red OT no está completamente segregada de la red corporativa.
Falta de Respuesta a Incidentes	No hay un plan de respuesta a incidentes específico para OT. No hay un equipo de respuesta a incidentes dedicado.
Gestión de Vulnerabilidades Deficiente	No hay una gestión activa de las vulnerabilidades. Los parches solo se aplican por indicación del proveedor.
Infraestructura Insegura	La VLAN 1 está en uso. No hay protecciones contra ataques "man-in-the-middle". Los switches de la planta de pasta son físicamente inseguros. Se ha descubierto un switch desconocido.
Falta de Gestión Centralizada	No hay una gestión centralizada de los equipos OT.

	Las configuraciones y actualizaciones de firmware se realizan manualmente.
Prácticas Inseguras	No hay políticas de contraseñas definidas. Se utilizan contraseñas locales en muchos dispositivos. Los protocolos innecesarios están habilitados. La segregación dentro de la red OT es limitada.
Vulnerabilidades Conocidas	Se detectaron vulnerabilidades en switches, routers y PLC.

Se presenta una tabla exhaustiva que detalla minuciosamente las vulnerabilidades detectadas en el sistema, acompañadas de sus respectivos planes de remediación. Para cada vulnerabilidad, se especifica su nivel de gravedad y el esfuerzo necesario para implementar una solución efectiva por parte del responsable. Esta clasificación meticulosa es vital para establecer un orden de prioridad en las acciones de mitigación, permitiendo así una asignación de recursos más eficiente y una respuesta rápida ante los riesgos más críticos. Al entender la magnitud y la complejidad de cada vulnerabilidad, las partes interesadas pueden tomar decisiones informadas para fortalecer la seguridad y mantener la integridad de la red. Este enfoque proactivo no solo ayuda a prevenir incidentes de seguridad potenciales, sino que también fomenta una cultura de vigilancia y mejora continua en el manejo de la infraestructura tecnológica. A continuación, se muestra el detalle en la **Tabla 6**.

Tabla 6

Vulnerabilidades y hallazgos

#	Observación / Vulnerabilidad / Riesgo	Implicación	Plan de Remediación.	Gravedad	Esfuerzo para remediar	Responsable
1	**Sin visibilidad, registro ni supervisión:** No se recopilan registros de ningún sistema que no sea el firewall. No hay visibilidad del tráfico de red y no se conoce una buena línea de base. * Red ICS La visibilidad y supervisión es uno de los 5 controles críticos de ciberseguridad de ICS.	• Será difícil detectar o responder a un ataque o incidente sin ninguna visibilidad. • No hay capacidad de revisar la información histórica para determinar lo que ha ocurrido en el pasado. • No es posible identificar amenazas o anomalías.	• Implementar una capacidad de supervisión pasiva de la red para establecer una línea de base de la red, identificar vulnerabilidades y detectar anomalías. • Habilitar el registro y recopilar los registros de todos los sistemas (Windows, PLC, infraestructura) en una ubicación central (por ejemplo, syslogserver).	Alta	Medio	Administrador red OT
2	**Inventario manual de activos de hardware y software:** Aunque existe un inventario de activos, se mantiene manualmente.	• Las protecciones podrían no aplicarse a todos los activos, si no se tienen identificados todos ellos. • Cuando no se conocen todos los activos, la respuesta a	• Utilizar una herramienta de supervisión pasiva para ayudar a establecer un inventario de activos automatizado y en tiempo real. • Ampliar con información de	Alta	Medio	Administrador red OT

		incidentes es difícil. • Las desviaciones de la norma son difíciles de detectar cuando no se conocen los activos".	Active Directory, cortafuegos y sistemas antivirus.			
3	**Las copias de seguridad se realizan manualmente:** Se realizan copias de seguridad de todos los sistemas, sin embargo, las copias de seguridad del firmware y la configuración de OT son manuales.	• El personal puede olvidarse de hacer copias de seguridad y puede que no se hagan después de cada cambio. • Con personal múltiple, las copias de seguridad pueden ser realizadas de forma diferente por diferentes personal. • Las copias de seguridad pueden no almacenarse de forma segura.	• Automatizar las copias de seguridad en la medida de lo posible. • Algunos proveedores de OT proporcionan capacidades de copia de seguridad automatizadas. • Crear secuencias de comandos para automatizar las copias de seguridad. • Asegurar que se realizan copias de seguridad tanto del firmware como de la configuración.	Alta	Medio	Administrador de Infraestructura
4	**Las copias de seguridad no son inmutables:** Las copias de seguridad se duplican en el centro de datos	• Los datos de ambos centros de datos podrían perderse debido a errores humanos, ransomware o sucesos del mundo real.	• Crear copias de seguridad "inmutables" escribiendo en un soporte externo y almacenándolo fuera de las	Alta	Medio	Administrador de Infraestructura

	de recuperación, pero no hay copias offline.		instalaciones y/o realizando una copia de seguridad en la nube.			
5	**Active Directory no ha sido reforzado:** Los sistemas OT Windows se gestionan con Active Directory, sin embargo, Active Directory no ha sido reforzado.	• Active Directory presenta una superficie de ataque muy grande que los atacantes tienen práctica en comprometer. • Si se compromete Active Directory, es probable que se comprometan TODOS los sistemas OT.	• Que un experto revise la configuración de Active Directory y aplique las mejores prácticas de seguridad. • Asegurar que Active Directory sea gestionado en adelante por personal con experiencia y conocimientos, posiblemente personal informático.	Alta	Medio	Encargado de Active Directory
6	**La configuración de los end point de Windows no está reforzada:** Los servidores y PC de trabajo Windows no tienen una configuración de base segura.	• Si un atacante consiguiera acceder al entorno OT, sería fácil comprometer los sistemas Windows y pasar de uno a otro.	• Desarrollar una imagen ISO base segura y utilizarla para aprovisionar todos los sistemas Windows.	Alta	Medio	Encargado de Aplicaciones Sistemas

7	**La configuración de los dispositivos de red no está reforzada:** El registro no está habilitado, los puertos no utilizados y los servicios web no están deshabilitados. Algunos switches no tienen autenticación configurada.	• Los dispositivos de red controlan todos los accesos a los sistemas de OT. Un ataque a la infraestructura de red, puede poner en peligro todo el entorno OT. • Sin registro ni supervisión, no es posible detectar un ataque contra la infraestructura de red.	• Desarrollar una configuración de base segura para la infraestructura de red, como los conmutadores, y asegurarse de que se aplica a todos los dispositivos. • Desactivar periódicamente los puertos no utilizados. • Implementar la autenticación centralizada. • Habilitar el registro y recopile los registros de forma centralizada	Alta	Medio	Encargado de Infraestructura
8	**La red OT no está completamente segregada de la red corporativa:** Se permite cierta comunicación SCADA-PCS-GR_01 directamente a CORPORATE-LPE_LIMS_01. * La Arquitectura Defendible es	• Toda comunicación entre las redes de TI y OT debe pasar a través de una DMZ. Al permitir la comunicación directa, es más probable que un agente de amenazas pueda establecer una conexión completa de mando y control desde la red OT a	•Replicar datos desde la red OT a un servidor en la DMZ y vuelva a replicarlos en la red corporativa. No permitir la comunicación directa entre las redes OT e IT	Alta	Alto	Encargado de Infraestructura

	uno de los 5 Controles Críticos de Ciberseguridad ICS	Internet a través de la red corporativa.			
9	**No existe un plan de respuesta a incidentes específico para OT:** Existe un plan corporativo de respuesta a incidentes, pero la personalización y las pruebas en OT son limitadas. No existe un retenedor de Respuesta a Incidentes (IR). * La Respuesta a Incidentes es uno de los 5 Controles Críticos de Ciberseguridad ICS".	• La respuesta dependería de que el personal disponible tome las medidas adecuadas. • El apoyo externo puede ser difícil de obtener sin un anticipo o un plan establecido con los proveedores. • La contención, erradicación y recuperación pueden llevar más tiempo del previsto debido a la falta de práctica. • Pueden surgir retos inesperados durante la respuesta.	• Desarrollar un plan de respuesta a incidentes específico para OT. • Establecer un Retenedor IR con un tercero de confianza. • Trabaje con los proveedores para entender cómo pueden ayudar. • Realice ejercicios de simulación para probar y mejorar el plan.	Alta	Alto	Encargado de Aplicaciones Sistemas
10	**Gestión de vulnerabilidades y parches limitada:** Los parches sólo se aplican por indicación del proveedor. No hay una gestión activa de las	• Si un atacante obtuviera acceso a cualquier sistema OT, probablemente podría elevar privilegios y obtener un acceso significativo al entorno.	• Adquirir o desarrollar una capacidad para identificar vulnerabilidades de OT, por ejemplo, a través de la monitorización pasiva.	Alta	Alto	Encargado de Aplicaciones Sistemas

	vulnerabilidades. * La Gestión de Vulnerabilidades Basada en Riesgos es uno de los 5 Controles Críticos de Ciberseguridad ICS	• La organización no es consciente de su exposición actual al riesgo debido a la falta de información.	• Crear un proceso para parchear periódicamente los sistemas menos sensibles, como Active Directory, estaciones de trabajo seleccionadas y servidores de archivos.			
11	**Las mejores prácticas de configuración de la infraestructura de red se aplican de forma incoherente:** La VLAN 1 está en uso, no hay protecciones habilitadas contra ataques machine-in-the-middle y otros.	• Varios ataques son más fáciles de ejecutar cuando se utiliza la VLAN 1. • Los ataques a nivel de red (por ejemplo, machine-in-the-middle) son más fáciles de llevar a cabo cuando las protecciones no están activadas.	• Durante el próximo turno o ventana de interrupción, cambiar la VLAN 1 a una VLAN diferente. • Habilitar protecciones como gratuitous arp protection y dhcp snooping".	Media	Alto	Encargado de Infraestructura
12	**La gestión de las infraestructuras corre a cargo de los técnicos de instrumentación y control:** Los técnicos no tienen formación en infraestructuras y no disponen del tiempo	• Sin formación y experiencia especializadas, los técnicos no tendrán los conocimientos profundos y la experiencia necesarios para proteger adecuadamente las redes y la infraestructura. • Incluso cuando tengan	• Asignar formalmente tiempo para el apoyo a la infraestructura, contratando personal adicional o aprovechando el personal de TI si es necesario.	Media	Alto	Encargado de Infraestructura

	necesario para gestionar toda la infraestructura.	conocimientos, sin tiempo para dedicar a la gestión de la infraestructura, muchas tareas básicas de configuración y seguridad no se completarán.				
13	**Se depende de los conocimientos no documentados que poseen los recursos clave:** Se confía mucho en los conocimientos del Administrador OT sobre el entorno que no están formalmente documentados.	• Si el Administrador OT dejara la organización o no estuviera disponible por cualquier otro motivo, se perdería una gran cantidad de conocimientos. • Podría resultar difícil recuperar o actualizar algunos sistemas y dispositivos si el Administrador OT no está disponible.	• Asignar tiempo para que el personal documente sus conocimientos. • Realizar ejercicios en los que el administrador no pueda contribuir para validar y aumentar los conocimientos de los demás. • Rotar responsabilidades para que otros puedan adquirir conocimientos cruzados.	Alta	Medio	Administrador red OT
14	**Las políticas de contraseñas no están definidas ni se aplican:** No hay una política de contraseñas definida para los dispositivos OT. Las contraseñas locales se utilizan en muchos	• Los usuarios pueden elegir contraseñas débiles que pueden ser adivinadas por un atacante. • Los usuarios que abandonan la organización pueden conservar las contraseñas de acceso.	• Siempre que sea posible, autentificarse en un directorio central que pueda aplicar la política de contraseñas. - Documentar una política de contraseñas sólida y	Alta	Medio	Encargado de Active Directory

	sistemas como la infraestructura de red y los PLC.	• No es posible rastrear o correlacionar acciones a un individuo cuando las cuentas son compartidas.	responsabilizar a los usuarios de su cumplimiento.			
15	**No hay gestión centralizada de los equipos OT:** La configuración de los controladores se gestiona dispositivo por dispositivo. Las actualizaciones de firmware se aplican manualmente.	• Los dispositivos pueden ejecutar software no actualizado. • Es difícil detectar cambios malintencionados en la configuración o el firmware. • Es más difícil mantener una versión de software y una configuración. • La exposición a los ataques aumenta cuando hay varias versiones diferentes y desactualizadas de software o firmware en uso.	• Determinar si el proveedor (por ejemplo, Schneider) ofrece capacidades de gestión y aprovéchelas si están disponibles. • Utilizar registros o secuencias de comandos sencillas para realizar un seguimiento del firmware y la configuración y detectar cambios.	Media	Alto	Encargado de Aplicaciones Sistemas
16	**Los switches de la planta de pasta son físicamente inseguros y carecen de**	• Puede producirse un apagón si el rack se cae o si los dispositivos fallan debido a las vibraciones, el	• Asegurar el rack. • Limpiar los dispositivos con la mayor frecuencia posible y	Media	Bajo	Encargado de Infraestructura

	autenticación de inicio de sesión: No se requiere autenticación para acceder a los conmutadores, la sala donde se encuentran no está cerrada con llave y su bastidor está separado de la pared.	polvo o la suciedad. • Cualquier persona que tenga acceso físico a la planta, puede usar la infraestructura de red para acceder a todos los sistemas de la red.	explore opciones para proporcionar protección adicional. • Exigir autenticación para iniciar sesión en los dispositivos y para entrar en la sala.			
17	**Se ha descubierto un switch desconocido y no gestionado:** Su propósito no está claro y la personal in situ no puede acceder al switch.	• El personal no dispone de un inventario completo. • Si el interruptor fallara, podría ser difícil sustituirlo con precisión. • El interruptor no está siendo actualizado y por lo tanto, podría estar sujeto a vulnerabilidades	• Obtener acceso al switch y gestionarlo junto a otros conmutadores. • Auditar periódicamente la red tanto física como electrónicamente (por ejemplo, CDP) para detectar dispositivos desconocidos.	Media	Bajo	Encargado de Infraestructura
18	**No se utiliza la tecnología de contraseñas seguras:** En muchos dispositivos se utilizan contraseñas locales. Estas contraseñas no se	• Las contraseñas elegidas pueden ser más débiles de lo óptimo si hay que recordarlas. • No hay forma segura de compartir contraseñas entre usuarios.	• Implementar algún tipo de tecnología de seguridad de contraseñas, como Secure Server o incluso Keypass.	Media	Bajo	Encargado de Active Directory

	almacenan de forma segura en una ubicación central	• Las contraseñas serán conocidas por los usuarios, mientras que algunas cajas fuertes de contraseñas pueden iniciar sesión sin revelar las contraseñas. • No hay forma de que otros determinen las contraseñas si el personal con conocimiento de las contraseñas no está disponible.				
19	**Los protocolos innecesarios están habilitados:** Protocolos como IPv6 que un atacante podría aprovechar en un ataque están habilitados.	•Los atacantes pueden aprovecharse de estos protocolos para interceptar y modificar la comunicación, y controlar la vista de red de los dispositivos.	• Desactivar IPv6, DHCPv6, LLMNR, WPAD, SSDP y NBNS a menos que sea necesario.	Media	Bajo	Encargado de Infraestructura
20	**Segregación limitada dentro de la red OT:** Aunque la red de procesos está separada de la red SCADA, hay muchos servidores ulti-homed	• Aunque las redes están separadas, el compromiso de un solo servidor podría permitir a un atacante atravesar las redes. • Con acceso a un único sistema	• En lugar de servidores de doble destino, conéctelos a una sola red e implante un cortafuegos entre las redes para controlar y supervisar activamente la	Media	Medio	Encargado de Infraestructura

	que sirven de puente entre ambas. No hay segmentación dentro de la red SCADA, donde se conectan sistemas con muchos propósitos diferentes. * La Arquitectura Defendible es uno de los 5 Controles Críticos de Ciberseguridad ICS".	de la red SCADA, un atacante puede interactuar con todos los demás sistemas SCADA y, a través de ellos, con la red de control de procesos.	comunicación. • Segmentar aún más la red SCADA para proporcionar un mayor control y visibilidad. Por ejemplo, coloque los sistemas de almacenamiento, Active Directory, SCADA e Ingeniería en subredes dedicadas protegidas por un cortafuegos.			
21	**Vulnerabilidades conocidas:** Se detectaron vulnerabilidades conocidas en switches y routers Cisco, así como en algunos PLC de Schneider. * La gestión de vulnerabilidades basada en el riesgo es uno de los 5 Controles de Ciberseguridad Críticos para ICS".	• Existen exploits que podrían utilizarse para tomar el control de la infraestructura de red si un atacante puede acceder a la red. • Pueden existir otros fallos operativos que podrían causar una interrupción.	• Documentar y realice un seguimiento de las versiones de software actuales y de las vulnerabilidades conocidas. • Actualizar los dispositivos de red siempre que sea posible, especialmente donde hay vulnerabilidades conocidas.	Media	Alto	Encargado de Infraestructura

CONCLUSIONES

El uso de las herramientas adecuadas, permitió una identificación precisa y completa de las vulnerabilidades y riesgos presentes en la red OT. En este caso, los sensores de Nozomi Networks, se destacaron como la solución ideal gracias a su tecnología específica para redes con tecnología operativa. Su naturaleza y diseño les permite integrarse sin problemas a este tipo de entornos, brindando una visibilidad profunda y granular de los activos y las comunicaciones.

La elaboración de una matriz de riesgos, vulnerabilidades y ponderación permitió realizar un análisis exhaustivo y preciso para determinar las áreas de mayor criticidad que requieren atención inmediata. En este proceso, la priorización de los cinco controles críticos para redes de sistemas de control industrial, constituye un pilar fundamental para garantizar la remediación completa de las vulnerabilidades detectadas.

El diseño de un plan efectivo para abordar vulnerabilidades y riesgos en redes OT, comienza con la priorización de las medidas de seguridad, esto es esencial para proteger la infraestructura crítica. Utilizar una matriz de ponderación de vulnerabilidades es clave para clasificar y ordenar las amenazas según su gravedad, probabilidad de explotación y esfuerzo de mitigación. Este enfoque permite usar recursos en las áreas de mayor riesgo primero. El plan de remediación debe incluir estrategias específicas para cada vulnerabilidad, actualizaciones de sistemas, fortalecimiento de políticas de seguridad, segmentación de la red, enfatizando la importancia de una cultura de seguridad. Además, es vital mantener el plan actualizado frente a nuevas amenazas y cambios tecnológicos, asegurando así una defensa robusta y adaptable para la red OT.

La credibilidad de un plan propuesto, se refuerza significativamente cuando un experto en la materia lo evalúa y aprueba para su creación o implementación. Aunque el plan se fundamente en las mejores prácticas, la perspectiva y el conocimiento profundo que ofrece un profesional con experiencia diaria en el campo añade un valor inestimable. Este aval no solo asegura una mayor fiabilidad en el enfoque propuesto, sino que también enriquece el plan con la sabiduría y las lecciones aprendidas que solo pueden proporcionar aquellos que manejan estos temas de manera cotidiana.

RECOMENDACIONES

Las investigaciones futuras deberían explorar la integración de tecnologías adicionales con los sensores de Nozomi Networks, evaluando su interoperabilidad y su potencial para mejorar aún más la detección de vulnerabilidades en las redes OT. Se recomienda diagnosticar nuevos problemas que puedan surgir al implementar estas soluciones en diferentes entornos operativos, identificando desafíos específicos y oportunidades de mejora. La difusión y socialización de los resultados obtenidos a través de estas herramientas es fundamental, destacando casos de éxito y su impacto en la ciberseguridad para promover su adopción en la industria.

En próximas investigaciones podrían centrarse en mejorar la matriz de riesgo, vulnerabilidad y encontrar formas de combinar la inteligencia artificial y el aprendizaje automático para automatizar y mejorar este proceso. Se recomienda evaluar los nuevos desafíos que surgen al utilizar esta matriz en diferentes entornos, para poder adecuar y adaptar la herramienta a diferentes tipos de redes OT. La socialización de cómo la matriz facilita una gestión de riesgos más efectiva, puede motivar a otras organizaciones a adoptar prácticas similares, resaltando la importancia de compartir metodologías y resultados para reforzar la seguridad en el sector.

Promover la divulgación de casos de estudio y análisis de impacto derivados de la implementación del plan, puede servir como herramienta de concienciación sobre la importancia de una cultura de seguridad robusta y adaptativa.

Es recomendable documentar y analizar los problemas identificados por expertos durante la revisión de planes, con el fin de desarrollar un marco de buenas prácticas para la elaboración y validación de futuras propuestas.

La socialización de la importancia de la validación experta en la creación e implementación de planes de seguridad, puede fomentar una mayor colaboración interdisciplinaria y elevar los estándares de calidad en la industria.

BIBLIOGRAFÍA

Acurio, S., & Moya, C. (2023). *PUCE Sede Ambato.* Repositorio PUCESA: https://repositorio.pucesa.edu.ec/bitstream/123456789/4088/1/79247.pdf

Canvia. (17 de 08 de 2023). *CANVIA*. https://www.canvia.com/redes-ot/

Castro, L. (5 de 3 de 2024). Matriz de validación. Quito, Pichincha, Ecuador.

Center for Internet Security. (2021). *https://learn.cisecurity.org/.* CIS Controls: https://learn.cisecurity.org/CIS-Controls-v8-Spanish-PDF

Centro para la Seguridad de Internet. (2024). *Centro para la Seguridad de Internet*. https://www.cisecurity.org/controls/v8

Cerón, D. (6 de 3 de 2024). Matriz de validación. Quito, Pichincha, Ecuador.

Chicaiza, D., & Torres, C. (01 de 2020). *Univesidad Técnica de Ambato.* Repositorio digital: https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

Engine, M. (2023). *www.manageengine.com/*. https://www.manageengine.com/latam/controles-de-seguridad-critica-cis.html

Erbes, A., Gutman, G., Lavarello , P., & Robert, V. (2019). *repositorio.cepal.org.* repositorio.cepal.org: https://repositorio.cepal.org/server/api/core/bitstreams/a03ff417-5eac-479e-969b-080466df1e47/content

Factory, O. C. (Dirección). (2019). *Webinar: La Seguridad en Entornos IT / OT* [Película].

Fortinet. (2023). *Fortinet*. https://www.fortinet.com/lat/solutions/industries/scada-industrial-control-systems/what-is-ot-security

Francés, J. (20 de 06 de 2022). *Universidad Politécnica de Catalunya.* BARCELONATECH: https://upcommons.upc.edu/bitstream/handle/2117/370900/172255.pdf

Gallegos, J. (6 de 3 de 2024). Matriz de validación. Quito, Pichincha, Ecuador.

Gary, T. (29 de junio de 2018). *Tenable*. https://www.tenable.com/blog/cis-adapts-critical-security-controls-to-industrial-control-systems

Gonçalves, L. (15 de septiembre de 2023). *adaptmethodology*. https://adaptmethodology.com/es/que-es-la-metodologia-agil/

Industrias, G. (2023). *industriasgsl*. https://industriasgsl.com/blogs/automatizacion/que-es-un-sistema-de-control-industrial

M. Lee, R., & Conway, T. (10 de 2022). *SANS.* The Five ICS Cibertsecurity Critical Controls: https://sansorg.egnyte.com/dl/R0r9qGEhEe

Mendoza, M. (28 de diciembre de 2021). *openaccess.uoc.edu.* openaccess.uoc.edu: https://openaccess.uoc.edu/bitstream/10609/138706/6/ascattonTFM1221memoria.pdf

Morgan, J. (1 de Octubre de 2020). *Indutrial Defender*. Indutrial Defender: https://www.industrialdefender.com/blog/establishing-ot-cybersecurity-fundamentals-cis-controls

Nozomi Networks. (2024). *Nozomi Networks*. https://es.nozominetworks.com/

Pirosanto, P. (26 de 06 de 2019). *DIGITEZEME*. https://www.digitizeme.blog/digitizeme-latam/redes-ot-qu%C3%A9-son-y-c%C3%B3mo-se-protegen-con-ciberseguridad

Quiroga, S. (22 de 05 de 2021). *Universidad Nacional Abierta y a Distancia UNAD de Colombia.* https://repository.unad.edu.co/bitstream/handle/10596/40838/smquirogad.pdf

SANS, I. (07 de 2022). *Instituto SANS*. https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

Scatton, A. (28 de 12 de 2021). *Universidad Poltécnica de Catalunya.* https://openaccess.uoc.edu/bitstream/10609/138706/6/ascattonTFM1221memoria.pdf

Tutomaniac. (2023). *TUTOMANIAC.* https://tutomaniac.com/que-es-la-piramide-de-la-automatizacion/

Unidas, N. (2024). *Naciones Unidas en Ecuador*. https://ecuador.un.org/es/sdgs

ANEXOS

ANEXO 1

ENTREVISTA

Entrevistador: Buenos días. Gracias por concedernos esta entrevista. Para comenzar, ¿podría explicarnos cuál es su rol en la empresa y cómo impacta la red OT en las operaciones mineras?

Encargado OT: Buenos días. Soy el encargado de la red de Tecnología Operativa aquí en la Mina. Mi trabajo es asegurar que todos los sistemas de control y automatización funcionen de manera óptima. La red OT es vital para nuestras operaciones mineras ya que controla desde la maquinaria pesada hasta los sistemas de ventilación y seguridad. Su buen funcionamiento es esencial para la eficiencia y seguridad de nuestras operaciones.

Entrevistador: Entendido. Recientemente, ¿han identificado vulnerabilidades en su red OT que podrían comprometer la seguridad o la eficiencia de las operaciones?

Encargado OT: Sí, hemos realizado una evaluación de seguridad cibernética a través de la contratación de un especialista que vino a la mina durante una semana y hemos identificado varias vulnerabilidades que necesitan ser abordadas. El detalle está en el informe que le entregue.

Entrevistador: ¿Cuál es el plan para remediar estas vulnerabilidades? ¿Podría detallar las etapas o acciones principales?

Encargado OT: Bueno. La verdad es que todavía no tenemos un plan de remediación, de hecho, justamente queríamos ver quien nos puede apoyar con eso para revisar su futura implementación en caso de resultar aprobada.

Entrevistador: ¿Cómo aseguran la continuidad de las operaciones mientras implementan estas medidas?

Encargado OT: Es algo complejo, pero planificamos las implementaciones para momentos de bajo impacto en las operaciones, y en algunos casos, establecemos sistemas temporales para garantizar que las operaciones críticas continúen sin interrupciones. Además, capacitamos constantemente a nuestro personal en prácticas de seguridad informática básicas para minimizar errores humanos.

Entrevistador: ¿Cómo planean mantener la seguridad de la red OT a largo plazo después de remediar las vulnerabilidades actuales?

Encargado OT: Eso va a depender de las recomendaciones que nos den los expertos en este tema o de quien realice el plan.

Entrevistador: ¿Cuál fue la razón para que busquen revisar la seguridad de su red OT?

Encargado OT: El corporativo nos solicitó hacerlo, parece que necesitan cumplir con ciertos requisitos para obtener una certificación internacional, parte de eso también es cumplir con los estándares que otras minas de otros países ya tienen. Solo nos estamos alineando, pero obviamente también nos queremos proteger de mejor manera, hoy día se escuchan tantos temas de amenazas en todo el mundo, no queremos caer en eso.

Entrevistador: Entiendo, siempre es prudente estar un paso delante de estos temas y no esperar a que sucedan para hacer algo.

Encargado OT: Por supuesto que sí.

Entrevistador: Para concluir, ¿cuál es el mensaje que le gustaría transmitir a otras empresas sobre la importancia de la seguridad de la red OT?

Encargado OT: La seguridad de la red OT no solo es vital para la protección contra amenazas cibernéticas, sino también para la continuidad y eficiencia de las operaciones. Invertir en seguridad informática es invertir en el futuro de la empresa. No esperen a ser víctimas de un ataque para empezar a tomar acciones. La prevención y la preparación son fundamentales.

Entrevistador: Muchas gracias por compartir con nosotros su enfoque y estrategias para mantener segura la red OT de su empresa. Su retroalimentación es valiosa para nuestro trabajo.

Encargado OT: Ha sido un gusto. Gracias por la apertura y oportunidad de discutir sobre este tema, nos servirá mucho su punto de vista.

ANEXO 2

FORMATO MATRIZ DE VALIDACIÓN

Matriz de Validación

Objetivo: Evaluar la viabilidad y eficacia de la PROPUESTA DE PLAN DE SEGURIDAD INFORMÁTICA PARA SISTEMA DE CONTROL INDUSTRIAL MEDIANTE LINEAMIENTOS DEL CENTRO PARA LA SEGURIDAD DE INTERNET

Criterios de Validación:

Criterio	Descripción	Ponderación	Evidencia	Resultado
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable / No aceptable
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable / No aceptable
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable / No aceptable
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	Aceptable / No aceptable

Escala de Resultados:

- **Aceptable:** Cumple con el criterio de forma satisfactoria.
- **No aceptable:** No cumple con el criterio de forma satisfactoria.

En base a los criterios propuestos, por favor, emita su valoración a la siguiente PROPUESTA DE PLAN DE SEGURIDAD INFORMÁTICA PARA SISTEMA DE CONTROL INDUSTRIAL MEDIANTE LINEAMIENTOS DEL CENTRO PARA LA SEGURIDAD DE INTERNET.

#	Observación / Vulnerabilidad / Riesgo	Implicación	Plan de Remediación.	Gravedad	Esfuerzo para remediar
1	**Sin visibilidad, registro ni supervisión:** No se recopilan registros de ningún sistema que no sea el firewall. No hay visibilidad del tráfico de red y no se conoce una buena línea de base. * Red ICS La visibilidad y supervisión es uno de los 5 controles críticos de ciberseguridad de ICS.	• Será difícil detectar o responder a un ataque o incidente sin ninguna visibilidad. • No hay capacidad de revisar la información histórica para determinar lo que ha ocurrido en el pasado. • No es posible identificar amenazas o anomalías.	• Implementar una capacidad de supervisión pasiva de la red para establecer una línea de base de la red, identificar vulnerabilidades y detectar anomalías. • Habilitar el registro y recopilar los registros de todos los sistemas (Windows, PLC, infraestructura) en una ubicación central (por ejemplo, syslogserver).	Alta	Medio
2	**Inventario manual de activos de hardware y software:** Aunque existe un inventario de activos, se mantiene manualmente.	• Las protecciones pueden no aplicarse a todos los activos si no se conocen todos. • La respuesta a incidentes es difícil cuando no se conocen todos los activos. • Las desviaciones de la norma son difíciles de detectar cuando no se conocen los activos".	• Utilizar una herramienta de supervisión pasiva para ayudar a establecer un inventario de activos automatizado y en tiempo real. • Ampliar con información de Active Directory, cortafuegos y sistemas antivirus.	Alta	Medio

3	**Las copias de seguridad se realizan manualmente:** Se realizan copias de seguridad de todos los sistemas, sin embargo, las copias de seguridad del firmware y la configuración de OT son manuales.	• El personal puede olvidarse de hacer copias de seguridad y puede que no se hagan después de cada cambio. • Con personal múltiple, las copias de seguridad pueden ser realizadas de forma diferente por diferentes personal. • Las copias de seguridad pueden no almacenarse de forma segura.	• Automatizar las copias de seguridad en la medida de lo posible. • Algunos proveedores de OT proporcionan capacidades de copia de seguridad automatizadas. • Crear secuencias de comandos para automatizar las copias de seguridad. • Asegurar que se realizan copias de seguridad tanto del firmware como de la configuración.	Alta	Medio
4	**Las copias de seguridad no son inmutables:** Las copias de seguridad se duplican en el centro de datos de recuperación, pero no hay copias offline.	• Los datos de ambos centros de datos podrían perderse debido a errores humanos, ransomware o sucesos del mundo real.	• Crear copias de seguridad "inmutables" escribiendo en un soporte externo y almacenándolo fuera de las instalaciones y/o realizando una copia de seguridad en la nube.	Alta	Medio
5	**Active Directory no ha sido reforzado:** Los sistemas OT Windows se gestionan con Active Directory, sin embargo, Active Directory no ha sido reforzado.	• Active Directory presenta una superficie de ataque muy grande que los atacantes tienen práctica en comprometer. • Si se compromete Active Directory, es probable que se comprometan TODOS los sistemas OT.	• Que un experto revise la configuración de Active Directory y aplique las mejores prácticas de seguridad. • Asegurar que Active Directory sea gestionado en adelante por personal con experiencia y conocimientos, posiblemente personal informático.	Alta	Medio

6	**La configuración de los end point de Windows no está reforzada:** Los servidores y PC de trabajo Windows no tienen una configuración de base segura.	• Si un atacante consiguiera acceder al entorno OT, sería fácil comprometer los sistemas Windows y pasar de uno a otro.	• Desarrollar una imagen ISO base segura y utilizarla para aprovisionar todos los sistemas Windows.	Alta	Medio
7	**La configuración de los dispositivos de red no está reforzada:** El registro no está habilitado, los puertos no utilizados y los servicios web no están deshabilitados. Algunos switches no tienen autenticación configurada.	• Los dispositivos de red controlan todos los accesos a los sistemas de OT. Un ataque a la infraestructura de red puede poner en peligro todo el entorno OT. • Sin registro ni supervisión, no es posible detectar un ataque contra la infraestructura de red.	• Desarrollar una configuración de base segura para la infraestructura de red, como los conmutadores, y asegurarse de que se aplica a todos los dispositivos. • Desactivar periódicamente los puertos no utilizados. • Implementar la autenticación centralizada. • Habilitar el registro y recopile los registros de forma centralizada	Alta	Medio
8	**La red OT no está completamente segregada de la red corporativa:** Se permite cierta comunicación SCADA-PCS-GR_01 directamente a CORPORATE-LPE_LIMS_01. * La Arquitectura Defendible es uno de los 5 Controles Críticos de Ciberseguridad ICS	• Toda comunicación entre las redes de TI y OT debe pasar a través de una DMZ. Al permitir la comunicación directa, es más probable que un agente de amenazas pueda establecer una conexión completa de mando y control desde la red OT a Internet a través de la red corporativa.	•Replicar datos desde la red OT a un servidor en la DMZ y vuelva a replicarlos en la red corporativa. No permitir la comunicación directa entre las redes OT e IT	Alta	Alto

9	**No existe un plan de respuesta a incidentes específico para OT:** Existe un plan corporativo de respuesta a incidentes, pero la personalización y las pruebas en OT son limitadas. No existe un retenedor de Respuesta a Incidentes (IR). * La Respuesta a Incidentes es uno de los 5 Controles Críticos de Ciberseguridad ICS".	• La respuesta dependería de que el personal disponible tome las medidas adecuadas. • El apoyo externo puede ser difícil de obtener sin un anticipo o un plan establecido con los proveedores. • La contención, erradicación y recuperación pueden llevar más tiempo del previsto debido a la falta de práctica. • Pueden surgir retos inesperados durante la respuesta.	• Desarrollar un plan de respuesta a incidentes específico para OT. • Establecer un Retenedor IR con un tercero de confianza. • Trabaje con los proveedores para entender cómo pueden ayudar. • Realice ejercicios de simulación para probar y mejorar el plan.	Alta	Alto
10	**Gestión de vulnerabilidades y parches limitada:** Los parches sólo se aplican por indicación del proveedor. No hay una gestión activa de las vulnerabilidades. * La Gestión de Vulnerabilidades Basada en Riesgos es uno de los 5 Controles Críticos de Ciberseguridad ICS	• Si un atacante obtuviera acceso a cualquier sistema OT, probablemente podría elevar privilegios y obtener un acceso significativo al entorno. • La organización no es consciente de su exposición actual al riesgo debido a la falta de información.	• Adquirir o desarrollar una capacidad para identificar vulnerabilidades de OT, por ejemplo, a través de la monitorización pasiva. • Crear un proceso para parchear periódicamente los sistemas menos sensibles, como Active Directory, estaciones de trabajo seleccionadas y servidores de archivos.	Alta	Alto
11	**Las mejores prácticas de configuración de la infraestructura de red se aplican de forma incoherente:** La VLAN 1 está en uso, no hay	• Varios ataques son más fáciles de ejecutar cuando se utiliza la VLAN 1. • Los ataques a nivel de red (por ejemplo, machine-in-the-middle) son	• Durante el próximo turno o ventana de interrupción, cambiar la VLAN 1 a una VLAN diferente. • Habilitar protecciones como	Media	Alto

	protecciones habilitadas contra ataques machine-in-the-middle y otros.	más fáciles de llevar a cabo cuando las protecciones no están activadas.	gratuitous arp protection y dhcp snooping".		
12	**La gestión de las infraestructuras corre a cargo de los técnicos de instrumentación y control:** Los técnicos no tienen formación en infraestructuras y no disponen del tiempo necesario para gestionar toda la infraestructura.	• Sin formación y experiencia especializadas, los técnicos no tendrán los conocimientos profundos y la experiencia necesarios para proteger adecuadamente las redes y la infraestructura. • Incluso cuando tengan conocimientos, sin tiempo para dedicar a la gestión de la infraestructura, muchas tareas básicas de configuración y seguridad no se completarán.	• Asignar formalmente tiempo para el apoyo a la infraestructura, contratando personal adicional o aprovechando el personal de TI si es necesario.	Media	Alto
13	**Se depende de los conocimientos no documentados que poseen los recursos clave:** Se confía mucho en los conocimientos del Administrador OT sobre el entorno que no están formalmente documentados.	• Si el Administrador OT dejara la organización o no estuviera disponible por cualquier otro motivo, se perdería una gran cantidad de conocimientos. • Podría resultar difícil recuperar o actualizar algunos sistemas y dispositivos si el Administrador OT no está disponible.	• Asignar tiempo para que el personal documente sus conocimientos. • Realizar ejercicios en los que Jorge no pueda contribuir para validar y aumentar los conocimientos de los demás. • Rotar responsabilidades para que otros puedan adquirir conocimientos cruzados.	Alta	Medio

14	**Las políticas de contraseñas no están definidas ni se aplican:** No hay una política de contraseñas definida para los dispositivos OT. Las contraseñas locales se utilizan en muchos sistemas como la infraestructura de red y los PLC.	• Los usuarios pueden elegir contraseñas débiles que pueden ser adivinadas por un atacante. • Los usuarios que abandonan la organización pueden conservar las contraseñas de acceso. • No es posible rastrear o correlacionar acciones a un individuo cuando las cuentas son compartidas.	• Siempre que sea posible, autentificarse en un directorio central que pueda aplicar la política de contraseñas. - Documentar una política de contraseñas sólida y responsabilizar a los usuarios de su cumplimiento.	Alta	Medio
15	**No hay gestión centralizada de los equipos OT:** La configuración de los controladores se gestiona dispositivo por dispositivo. Las actualizaciones de firmware se aplican manualmente.	• Los dispositivos pueden ejecutar software no actualizado. • Es difícil detectar cambios malintencionados en la configuración o el firmware. • Es más difícil mantener una versión de software y una configuración. • La exposición a los ataques aumenta cuando hay varias versiones diferentes y desactualizadas de software o firmware en uso.	• Determinar si el proveedor (por ejemplo, Schneider) ofrece capacidades de gestión y aprovéchelas si están disponibles. • Utilizar registros o secuencias de comandos sencillas para realizar un seguimiento del firmware y la configuración y detectar cambios.	Media	Alto
16	**Los switches de la planta de pasta son físicamente inseguros y carecen de autenticación de inicio de sesión:** No se requiere autenticación para	• Puede producirse un apagón si el rack se cae o si los dispositivos fallan debido a las vibraciones, el polvo o la suciedad.	• Asegurar el rack. • Limpiar los dispositivos con la mayor frecuencia posible y explore opciones para proporcionar protección adicional.	Media	Bajo

	acceder a los conmutadores, la sala donde se encuentran no está cerrada con llave y su bastidor está separado de la pared.	• Cualquiera con acceso físico a la planta podría acceder a la infraestructura de red a través de la cual podría acceder a todos los sistemas de la red.	• Exigir autenticación para iniciar sesión en los dispositivos y para entrar en la sala.		
17	**Se ha descubierto un switch desconocido y no gestionado:** Su propósito no está claro y la personal in situ no puede acceder al switch.	• El personal no dispone de un inventario completo. • Si el interruptor fallara, podría ser difícil sustituirlo con precisión. • El interruptor no está siendo actualizado y por lo tanto podría estar sujeto a vulnerabilidades	• Obtener acceso al switch y gestionarlo junto a otros conmutadores. • Auditar periódicamente la red tanto física como electrónicamente (por ejemplo, CDP) para detectar dispositivos desconocidos.	Media	Bajo
18	**No se utiliza la tecnología de contraseñas seguras:** En muchos dispositivos se utilizan contraseñas locales. Estas contraseñas no se almacenan de forma segura en una ubicación central	• Las contraseñas elegidas pueden ser más débiles de lo óptimo si hay que recordarlas. • No hay forma segura de compartir contraseñas entre usuarios. • Las contraseñas serán conocidas por los usuarios, mientras que algunas cajas fuertes de contraseñas pueden iniciar sesión sin revelar las contraseñas. • No hay forma de que otros determinen las contraseñas si el	• Implementar algún tipo de tecnología de seguridad de contraseñas, como Secure Server o incluso Keypass.	Media	Bajo

		personal con conocimiento de las contraseñas no está disponible.			
19	**Los protocolos innecesarios están habilitados:** Protocolos como IPv6 que un atacante podría aprovechar en un ataque están habilitados.	•Los atacantes pueden aprovecharse de estos protocolos para interceptar y modificar la comunicación y controlar la vista de red de los dispositivos.	• Desactivar IPv6, DHCPv6, LLMNR, WPAD, SSDP y NBNS a menos que sea necesario.	Media	Bajo
20	**Segregación limitada dentro de la red OT:** Aunque la red de procesos está separada de la red SCADA, hay muchos servidores ulti-homed que sirven de puente entre ambas. No hay segmentación dentro de la red SCADA, donde se conectan sistemas con muchos propósitos diferentes. * La Arquitectura Defendible es uno de los 5 Controles Críticos de Ciberseguridad ICS".	• Aunque las redes están separadas, el compromiso de un solo servidor podría permitir a un atacante atravesar las redes. • Con acceso a un único sistema de la red SCADA, un atacante puede interactuar con todos los demás sistemas SCADA y, a través de ellos, con la red de control de procesos.	• En lugar de servidores de doble destino, conéctelos a una sola red e implante un cortafuegos entre las redes para controlar y supervisar activamente la comunicación. • Segmentar aún más la red SCADA para proporcionar un mayor control y visibilidad. Por ejemplo, coloque los sistemas de almacenamiento, Active Directory, SCADA e Ingeniería en subredes dedicadas protegidas por un cortafuegos.	Media	Medio

21	**Vulnerabilidades conocidas:** Se detectaron vulnerabilidades conocidas en switches y routers Cisco, así como en algunos PLC de Schneider. * La gestión de vulnerabilidades basada en el riesgo es uno de los 5 Controles de Ciberseguridad Críticos para ICS".	• Existen exploits que podrían utilizarse para tomar el control de la infraestructura de red si un atacante puede acceder a la red. • Pueden existir otros fallos operativos que podrían causar una interrupción.	• Documentar y realice un seguimiento de las versiones de software actuales y de las vulnerabilidades conocidas. • Actualizar los dispositivos de red siempre que sea posible, especialmente donde hay vulnerabilidades conocidas.	Media	Alto

Resultados:

Criterio	Descripción	Ponderación	Evidencia	Resultado	
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☐	☐
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☐	☐
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☐	☐
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☐	☐
Observaciones adicionales:					

Nombre del Especialista:	
Cédula:	
Firma:	

ANEXO 3

MATRICES DE VALIDACIÓN REVISADAS POR LOS TRES EXPERTOS

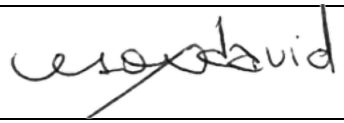
Resultados:

Criterio	Descripción	Ponderación	Evidencia	Resultado	
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				■	☐
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				■	☐
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				■	☐
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				■	☐
Observaciones adicionales:					

Nombre del Especialista:	Luis Enrique Castro Q.
Cédula:	171262634-8
Firma:	

Resultados:

Criterio	Descripción	Ponderación	Evidencia	Resultado	
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☑	☐
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☑	☐
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☑	☐
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	**Aceptable**	**No aceptable**
				☑	☐
Observaciones adicionales:					

Nombre del Especialista:	MSc. David Cerón
Cédula:	040130751-7
Firma:	

Resultados:

Criterio	Descripción	Ponderación	Evidencia	Resultado	
				Aceptable	**No aceptable**
Pertinencia	El plan aborda las necesidades específicas de una red OT y sus activos.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	☐	☐
				Aceptable	**No aceptable**
Eficacia	El plan incluye medidas de seguridad adecuadas para mitigar los riesgos identificados.	Alta	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	☐	☐
				Aceptable	**No aceptable**
Eficiencia	El plan se puede implementar con los recursos disponibles.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	☐	☐
				Aceptable	**No aceptable**
Factibilidad	El plan es viable desde el punto de vista técnico y operativo.	Media	Matriz de análisis de riesgos y vulnerabilidades con su plan de acción.	☐	☐
Observaciones adicionales:					

Nombre del Especialista:	Jaime José Gallegos Oleas
Cédula:	1713538286
Firma:	GALLEGOS OLEAS JAIME JOSE (AECUIO) Firmado digitalmente por GALLEGOS OLEAS JAIME JOSE (AECUIO) Fecha: 2024.03.06 18:01:58 -05'00'