ARQUITECTURA DE CIBERSEGURIDAD PARA INFRAESTRUCTURAS CRÍTICAS EN UNA EMPRESA DE PETRÓLEO Y GAS, BASADO EN LA ISA/IEC 62443-3-3

YURI LILIANA LOPEZ BOHORQUEZ
WILSON ARMANDO ROA MUÑOZ
WILSON DE JESUS GUEVARA GIL

Universidad de los Andes
Departamento de Ingeniería de Sistemas y Computación

{ y.lopezb - w.roam – w.guevara } @uniandes.edu.co

Resumen

Con el auge y crecimiento exponencial de las nuevas tecnologías de inteligencia artificial, el análisis y centralización de datos, el uso de la nube y la interconexión de redes para acceder fácilmente a la información, las empresas están buscando modernizar sus procesos y tecnología. Estos cambios requieren que las empresas inviertan en un marco de ciberseguridad robusto para proteger la información durante la transferencia, almacenamiento y el procesamiento.

Las empresas que tienen o administran infraestructuras críticas no son ajenas a este requerimiento. Las infraestructuras críticas son sistemas y activos vitales para una organización, su afectación o destrucción tendría un impacto devastador en la seguridad, economía, salud pública, entre otros aspectos. En este proyecto, se propuso evaluar la postura de ciberseguridad actual de la compañía objetivo, identificar amenazas a través de pruebas, observaciones y análisis de documentos, se seleccionó la norma ISA 62443 como marco de referencia para la protección de sistemas de control y automatización industrial (IACS), posteriormente, se realizó una evaluación de riesgos para identificar el estado actual de seguridad y seleccionar los controles de la norma que fortalecen la postura de ciberseguridad de la organización.

Palabras clave: OT, IACS, ISA62443, Ciberseguridad, Riesgos, Controles

Abstract

With the rise and exponential growth of new artificial intelligence technologies, the analysis and centralization of data, the use of the cloud and the interconnection of networks to easily access information, companies are looking to modernize their processes and technology. These changes require companies to invest in a robust cybersecurity framework to protect information during transfer, storage and processing.

Companies that own or manage critical infrastructures are no strangers to this requirement. Critical infrastructures are vital systems and assets for an organization; their affectation or destruction would have a devastating impact on security, economy, public health, among other aspects. In this project, it was proposed to evaluate the current cybersecurity posture of the target company, identify threats through tests, observations and document analysis, the ISA 62443 standard was selected as a reference framework for the protection of industrial automation and control systems (IACS), subsequently, a risk assessment was performed to identify the current state of security and select the controls of the standard that strengthen the cybersecurity posture of the organization.

Keywords: OT, IACS, ISA62443, Cybersecurity, Risks, Controls

I. CONTEXTO

En el contexto actual de creciente digitalización y dependencia de las tecnologías de la información, la ciberseguridad se ha convertido en un aspecto fundamental para garantizar la integridad, confidencialidad y disponibilidad de los activos críticos de las organizaciones. Especialmente en sectores críticos como el de petróleo y gas, las empresas enfrentan desafíos significativos en la protección de sus infraestructuras contra amenazas cibernéticas cada vez más sofisticadas y persistentes (Cerqueira Junior & Arima, 2023; Czachorowski et al., 2023; Kotsakis & Boukli, 2023).

Este trabajo se centra en generar e implementar controles de ciberseguridad específicamente diseñados para ser aplicados en sistemas de operación (OT) de infraestructuras críticas para una empresa del sector de petróleo y gas. El objetivo es fortalecer su postura de seguridad y mitigar los riesgos asociados a posibles ciberataques. Este proyecto se fundamenta en la imperativa necesidad de proteger los activos digitales y garantizar la continuidad operativa en un entorno altamente interconectado y expuesto a amenazas cibernéticas en constante evolución.

Mediante un enfoque multidimensional que incorpora las mejores prácticas, estándares y controles de seguridad pertinentes para la protección de sistemas de control y automatización industrial (IACS), se proporciona a las compañías una estructura coherente y efectiva para gestionar los riesgos de ciberseguridad, identificar vulnerabilidades en sus infraestructuras críticas y establecer mecanismos de respuesta ante posibles incidentes cibernéticos.

II. DESCRIPCIÓN DE LA PROPUESTA

A. Descripción del problema

Este proyecto parte de la necesidad de una compañía de petróleo y gas que ha visto el creciente número de ataques cibernéticos hacia infraestructuras similares alrededor del

mundo y la ausencia de definición e implementación de un marco de ciberseguridad robusto para proteger su propia tecnología; en caso de materializarse un evento de seguridad podría reflejarse en la pérdida de datos y la interrupción de sus operaciones, desencadenando pérdidas financieras y daño a la reputación.

Dentro de los eventos de seguridad más relevantes del sector tenemos.

- Febrero 2022, Terminales petroleras en instalaciones portuarias de Bélgica, Países Bajos y Alemania.
- Mayo del 2021, EE.UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país, disminuyendo y la demanda, especialmente de combustibles para vehículos y afectando la economía del país.
- Noviembre 2019, secuestro de datos de una petrolera mexicana.

Si esta compañía omite la implementación de un marco de ciberseguridad eficaz, es probable que sufra ataques cibernéticos, especialmente dado su plan de centralizar los datos de producción en la nube. Llegando a tener pérdidas de datos, interrupciones en la producción y posibles violaciones de las regulaciones de protección de datos.

En ese sentido, la implementación de un marco de ciberseguridad eficaz puede ayudar a proteger la infraestructura de futuros ataques cibernéticos, esto implica la adopción de estándares de seguridad reconocidos, la capacitación y concientización del personal en prácticas de seguridad, la realización de auditorías de seguridad regulares y la implementación de tecnologías de seguridad avanzadas. Además, se podría considerar establecer de forma interna o externa, un equipo de respuesta a incidentes de seguridad para manejar cualquier brecha de seguridad de manera efectiva.

B. Propuesta de solución

El objetivo general se basa en establecer la arquitectura y los controles de seguridad para una de las instalaciones de un sistema SCADA en una empresa de petróleo y gas; lo anterior, utilizando el framework ISA/IEC 62443-3-3 como base de los controles a seleccionar e implementar, el proceso incluye:

- Evaluación de la arquitectura de la red de procesos.
- Diagnóstico de ciberseguridad que permita identificar la postura actual de la infraestructura critica.
- Evaluación de riesgos basados en la ISO 27005.
- Identificación y selección de controles que contribuyan a mejorar la postura de ciberseguridad de la infraestructura.

Como resultado del ejercicio, se identificaron 43 controles que permitirán robustecer la seguridad de redes operativas desde varios frentes en la compañía y reducir riesgos al considerar toda su implementación, para llevarlo a cabo se diseñó un plan de trabajo a 21 meses en los que la compañía deberá cada 3 meses implementar, configurar y poner en producción, estos controles se encuentran encaminados tanto en tareas de gobierno como técnicas, buscando mejorar su postura de ciberseguridad y mitigar los riesgos asociados a su operación. El beneficio de este plan es que podrá ser implementado en cada una de sus instalaciones, permite un ciclo de mejora continua y el esfuerzo en la implementación de algunos de estos controles podrán aplicar a varias instalaciones, reduciendo tiempos de implementación y costos.

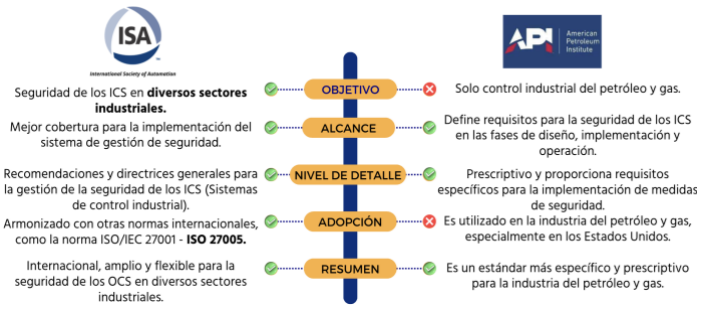
La propuesta de solución que presentamos en este proyecto genera una línea base de seguridad que puede ser implementada por cualquier empresa con sistema SCADA y es por el tipo de controles que deben partir las empresas a fortalecer sus sistemas de seguridad, sin embargo, la compañía objeto de este trabajo a futuro deberá mantener la gestión de riesgos planeada y evaluar los controles adicionales que presenta la norma ISA/IE 62443-3-3, los cuales aportan a mejorar el nivel de madurez de la seguridad implementada.

C. Metodología

Para el estudio de caso aplicado se empleó una metodología mixta que permitiera investigar detalles relacionados con la ciberseguridad en infraestructuras críticas. Se realizó una revisión exhaustiva de literatura y se analizaron textos y documentos para comprender los conceptos y teorías existentes de a algunos frameworks que permiten fortalecer la seguridad de las redes operativas (OT).

En este proceso de revisión, se compararon dos estándares elegibles para dar solución a la problemática expuesta: se trata de ISA/IEC 62443, y, API 1164 como se expone en la Figura 1. Además, se realizó una evaluación de riesgo que permitiera conocer el estado actual de la seguridad, lo que permitió la selección objetiva e implementación de controles de ciberseguridad basado en criterios predefinidos. Así mismo, se recopilaron y analizaron datos cuantitativos para medir la eficacia de estos. En resumen, el proyecto combinó enfoques cualitativos y cuantitativos con el objetivo de resolver un problema práctico en un contexto específico.

Figura 1
Comparación de los frameworks



Nota: Se toman las características principales de las normas para evaluar la opción mediante la cual se va a trabajar este proyecto. Fuente: Elaboración propia

III. SOLUCIÓN

Según Atkins and Lawson (2021), a pesar de los avances en las políticas de ciberseguridad para infraestructuras críticas, persisten tanto los éxitos como los fracasos. Esta observación sugiere que aún hay margen para mejorar en la implementación y el cumplimiento de estas políticas, a pesar de los avances en la tecnología y las políticas de ciberseguridad, todavía existen desafíos para la protección de las infraestructuras críticas, como la escasez de recursos, la resistencia al cambio y la falta de conciencia sobre las amenazas de seguridad.

Se encontró como producto del análisis de los estándares propuestos que, el estándar ISA/IEC 62443, desarrollado por la *Sociedad Internacional de Automatización (ISA)* y la Comisión *Electrotécnica Internacional (IEC)***, (**en comparación con API 1164), establece de manera más detallada un marco integral para la seguridad de los sistemas de automatización y control industrial en sectores como la energía, el agua y la industria. La implementación de la norma ISA/IEC 62443 puede ayudar a las empresas a reducir los costos a largo plazo al prevenir daños a la propiedad, pérdida de producción y el robo de datos.

El Framework ISA/IEC 62443, establece pasos generales que las organizaciones pueden seguir para evaluar su postura actual de seguridad y así definir los controles que le permitan mejorarla. Los pasos sugieren:

A. Definición del objetivo de la evaluación
B. Recolección de datos
C. Análisis de los datos
D. Desarrollo del plan de acción
E. Implementación del plan de acción
F. Revisión y actualización del plan

A continuación, se presenta el desarrollo de los pasos, es de aclarar que última actividad hace referencia a la ejecución del plan que deberá proyectar la compañía para garantizar la continuidad de las actividades definidas en este proyecto.

A. Definición del objetivo de la evaluación

Lo primero que debe hacer una organización es definir los objetivos de la evaluación de postura de ciberseguridad, esto ayudará a determinar el alcance de la evaluación y los tipos de datos que deben recopilarse.

Objetivo: Evaluar la arquitectura de la red de procesos y la topología de interconexión entre la red de tecnología operativa (TO) y la red de tecnología de la información (TI).

B. Recolección de datos

Seguido por la **recolección de datos** sobre sus activos, riesgos y controles de seguridad, lo anterior, utilizando métodos como entrevistas, encuestas, **escaneos de vulnerabilidades y pruebas de penetración**; basados en el proceso de recopilar datos enunciado en el marco 62443-3-3, utilizaremos la información suministrada por la compañía y realizamos una evaluación de vulnerabilidades que incluye una prueba de penetración pasiva (sin afectar la infraestructura operativa).

C. Análisis de los datos

Para este proceso se utilizó la información resultante, lo que nos permite identificar los riesgos de ciberseguridad más significativos y las áreas de mejora.

Se realizó una prueba tipo caja blanca para identificar vulnerabilidades, estas pruebas son una parte fundamental de evaluar el nivel de seguridad, confiabilidad y disponibilidad de los sistemas y activos críticos para la operación. En su ejecución se consideraron:

- El atacante tiene conocimiento completo del sistema objetivo, como funcionalidad, arquitectura y configuración.
- Se enfoca en encontrar vulnerabilidades en el diseño e implementación del sistema.
- Requiere acceso al código fuente y a la documentación del sistema.

Los resultados de las pruebas permitieron identificar múltiples deficiencias, dentro de las que se destacan fallos que se mapean a los siguientes controles, referenciados en el framework 62443-3-3:

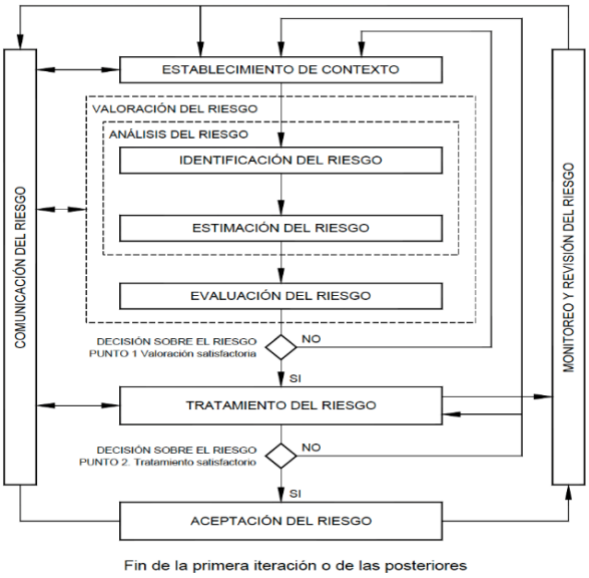
- RDF - Flujo de datos restringido – relacionado con fallas en la segmentación de la red.
- UC - Control de uso – con problemas de seguridad en el sistema de control de acceso a dispositivos.
- RA - Disponibilidad de recursos – asociado a ineficiencias en los controles de monitoreo y detección de intrusiones.

Los anteriores insumos fueron fundamentales para llevar a cabo un diagnóstico de ciberseguridad, el cual permitió identificar la postura actual del sistema en fase de estudio. Se sigue con un proceso de evaluación basado en la ISO27005, que adopta un enfoque integral en la gestión de riesgos de seguridad. Esta norma es fundamental para identificar, evaluar y mitigar riesgos de seguridad, abordando aspectos como la confidencialidad, integridad y disponibilidad de los activos críticos. La ISO27005 ofrece una metodología flexible y escalable que permite a las organizaciones evaluar y tratar los riesgos de seguridad de manera holística, integrando la gestión de riesgos en su cultura organizativa y procesos de negocio, asegurando una respuesta eficaz ante las amenazas.

La selección de ISO27005 permite alinear el proyecto con el marco de gestión de riesgos de seguridad establecido por la compañía, esto asegura una mayor coherencia y facilidad de adaptación del proyecto a los procesos ya establecidos en la gestión de riesgos de la organización. Además, ISO27005 es preferible por su naturaleza más generalizada y adaptable a una amplia gama de contextos organizativos, su flexibilidad y compatibilidad con otros estándares de seguridad de la

información son ventajas adicionales que hacen que sea una elección sólida para este proyecto.

Figura 2
Proceso de gestión del riesgo en la seguridad



Nota: La norma ISO27005 sugiere un flujo de actividades que permiten llevar a cabo la gestión integral de riesgos de seguridad. Fuente: Tomado de Norma Técnica Colombiana NTC-ISO/IEC 27005.

La Figura 2, ofrece una representación visual del proceso integral de gestión del riesgo en la seguridad, siguiendo las directrices establecidas por la norma. Este proceso consta de cuatro fases fundamentales, cada una de las cuales despliega un conjunto especifico de actividades destinadas a garantizar una evaluación exhaustiva y efectiva de riesgos:

- **Establecer el contexto**
- **Analizar los riesgos**
- **Evaluar los riesgos**
- **Tratar los riesgos**

La etapa de **establecer el contexto** implica definir el alcance y los objetivos del proceso de gestión del riesgo, así como identificar las partes interesadas y sus expectativas; la etapa de identificación de riesgos implica identificar los activos relevantes, se establecen los criterios de evaluación y se definen los límites de la evaluación.

El **analizar los riesgos** consiste en identificar, de manera sistemática, los riesgos que pueden afectar la seguridad de la información de la organización. Esto incluye identificar las amenazas, las vulnerabilidades y los impactos potenciales.

La etapa de **evaluar los riesgos** implica evaluar la probabilidad y el impacto en la organización de cada riesgo identificado, así como determinar el nivel de riesgo aceptable o si requiere medidas adicionales para tratarlos.

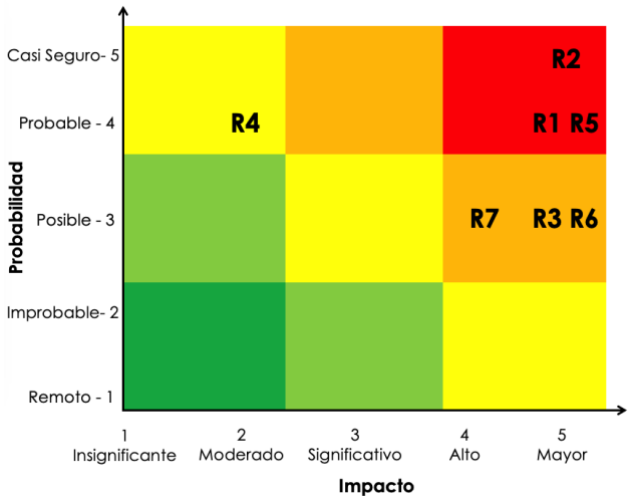
El **tratamiento de riesgos** implica seleccionar y aplicar las medidas de control adecuadas para reducir el nivel de riesgo a un nivel aceptable. Esto puede incluir la implementación de controles de seguridad, la transferencia de riesgos a terceros, la aceptación de riesgos o la eliminación de actividades de alto riesgo.

La gestión del riesgo en la seguridad incluye actividades de monitoreo y revisión que se ejecutan continuamente para garantizar que las medidas de control sean efectivas en el tiempo y permitan identificar nuevos riesgos.

La evaluación de riesgos nos permitió identificar 7 riesgos clave y 36 vulnerabilidades, dentro de los cuales podemos destacar:

- **R1 - Pérdida de la disponibilidad de la infraestructura critica**
- **R2 - Pérdida de la confidencialidad de la información**
- **R3- Pérdida de integridad en los datos que manejan los sistemas**
- **R4 - Interrupción en la conectividad entre IT y OT**
- **R5 - Pérdida de control sobre los elementos OT**
- **R6 - Impactos al entorno ambiental**
- **R7 - Pérdida de oportunidad por espionaje industrial.**

Figura 3
Mapa de riesgo inherente



Nota: Se grafican los riesgos según la medida de probabilidad e impacto. Fuente: Elaboración propia

La Figura anterior, que representa el mapa de riesgo inherente, es una herramienta visual clave en la gestión de la ciberseguridad en la industria del petróleo y gas; este mapa proporciona una representación gráfica de los diferentes niveles de riesgo inherente asociados con los escenarios de amenazas identificados, como la pérdida de disponibilidad de la infraestructura crítica, la pérdida de confidencialidad de los datos de la operación y la interrupción en la conectividad entre

IT y OT. Al categorizar los riesgos inherentes en función de su probabilidad e impacto, la organización puede identificar claramente las áreas de mayor vulnerabilidad y priorizar la implementación de medidas de mitigación y controles de seguridad. Este enfoque visual facilita la comprensión y comunicación de los riesgos cibernéticos, permitiendo a la empresa tomar decisiones estratégicas para fortalecer su postura de ciberseguridad y proteger sus activos críticos contra posibles amenazas.

Para tratar riesgos, se adoptó lo dispuesto en la norma ISO27005 que establece un enfoque sistemático, una vez identificados los riesgos expuestos la compañía, se definió el tratamiento, se estableció y evaluó la efectividad de los controles, a los que se les realizó una segunda evaluación.

Considerando el tipo de riesgo y causas asociadas, se evaluó el tratamiento (reducir, aceptar, transferir o evitar), considerando los criterios de aceptación y la respuesta definidos previamente.

Para cada causa vinculada a los riesgos identificados, se definió el plan de tratamiento específico basado en los controles específicos para redes OT que ofrece la ISA/IEC 624433-3-3 que permiten reducir tanto el impacto como la probabilidad asociada, esto puede implicar la implementación de controles internos adecuados o la transferencia del riesgo a un proveedor especializado.

Se presentó a la organización una visión detallada de las acciones necesarias para fortalecer la seguridad de la infraestructura crítica, proteger los activos, datos sensibles y garantizar la continuidad operativa en un entorno digitalmente interconectado. Al seguir este plan de tratamiento de riesgos, la empresa puede mejorar significativamente su postura de ciberseguridad y reducir la exposición a vulnerabilidades, demostrando un compromiso proactivo con la protección de la información y la infraestructura contra posibles ataques.

D. Desarrollo del plan de acción

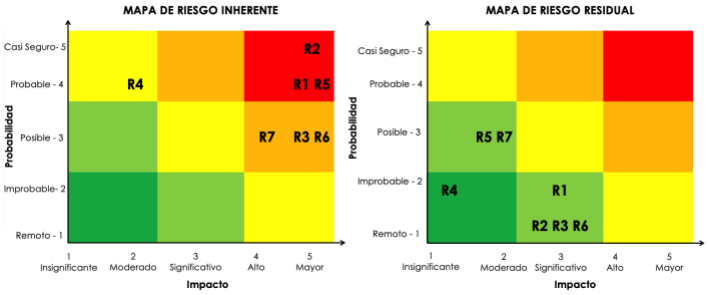
Para identificar y seleccionar controles que mejoren la postura de ciberseguridad de la infraestructura, se sustentó en la evaluación de riesgos y correlacionamos con la ISA 62443-3-3, que proporciona una guía detallada para la seguridad cibernética en sistemas de control industrial (SCI). Identificamos que su estructura en diferentes secciones cubre aspectos como la gestión de activos, la gestión de seguridad para el ciclo de vida del sistema, la seguridad de la red y la protección del sistema, entre otros.

La norma incluye múltiples controles que abordan los riesgos y amenazas asociados con la seguridad cibernética en los sistemas de control industrial. Con la información de los controles, su evaluación del diseño y el mapeo con cada riesgo, evaluamos nuevamente el riesgo para calcular un posible riesgo residual es decir el riesgo reducido al que se enfrenta la compañía una vez se lleve a cabo el desarrollo de todos los controles presentados en este proyecto. El cálculo residual se basa en una evaluación subjetiva basada en el resultado y comportamiento esperado tras la implementación del plan, y se considera la información y evidencia que se debe considerar para que la compañía mantenga la evaluación periódicamente.

Al evaluar el riesgo residual, se determina el nivel de riesgo que permanece después de aplicar los controles, lo que permite a la organización comprender mejor las áreas donde se requiere una mayor atención o mejora en términos de seguridad cibernética. Esta evaluación continua del riesgo residual es crucial para mantener una postura de ciberseguridad sólida y adaptativa, garantizando la protección de los activos críticos y la continuidad operativa en un entorno digital en constante evolución.

Como resultado de la definición de controles identificados y adaptados a las necesidades de la compañía y al tratamiento de los riesgos se calcula en la siguiente grafica como extremo, alto y medio, a un riesgo residual calificado como bajo y mínimo cuando se definen controles.

Figura 4
Mapa de calor del riesgo



Nota: Comparativo de la medición del riesgo inherente (sin controles) con el riesgo residual que tiene controles definidos para minimizar el impacto o la probabilidad. Fuente: Elaboración propia

La Figura anterior, representa el mapa de calor del riesgo, mediante una representación gráfica de la evaluación de riesgos inherentes y residuales, mostrando de manera clara y concisa la transición de los riesgos en función de su impacto y probabilidad.

E. Implementación del plan de acción

Para lograr la disminución presentada en el mapa de calor de riesgo residual, se presentó una sugerencia de implementación de 43 controles que mitigan los riesgos, se han definido basados en el contexto de la organización y la infraestructura identificada en el inventario de activos.

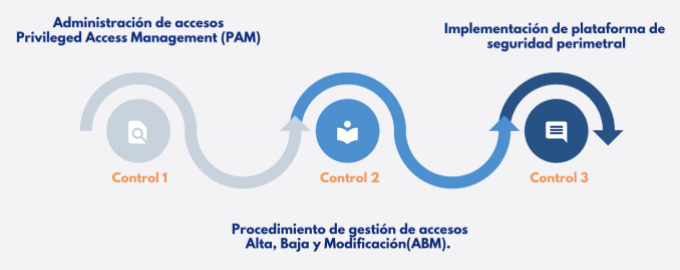
Según el análisis de los riegos inherentes, los siguientes 3 riesgos impactan desde distintos ángulos a la compañía, afectando la confidencialidad, disponibilidad e integridad, su materialización puede provocar gran afectación en diferentes contextos, tales como reputacional, económico, humano, ambiental y a nivel de clientes

- **R1: Pérdida de la disponibilidad de la infraestructura crítica**
- **R2: Pérdida de la confidencialidad de la información**
- **R5: Pérdida de control sobre los elementos OT**

Se estableció un plan que impacte directamente sobre estos, para lo cual se seleccionaron tres controles de la primera iteración, estos controles servirán de base para la implementación del plan completo de controles propuesto.

Para llevar a cabo este proyecto de la lista de 43 controles se establecieron e implementaron 3 controles que impactan directamente a los riesgos R1, R2 y R5 con mayor impacto a la compañía, estos 3 controles listados en la Figura 4 fueron desarrollados e implementados en la compañía como parte del desarrollo del plan de trabajo. A continuación, se desarrollan estos controles:

Figura 5
Controles implementados



Nota: Controles seleccionados de la norma ISA/IEC 62443-3-3 establecidos e implementados durante el proyecto. Fuente: Elaboración propia

A. Primer control

Matriz de roles y perfiles e implementación del PAM – R5

Para el desarrollo de este control, se propuso la definición de una matriz de roles y perfiles para identificar quienes deben tener acceso a los sistemas y los roles que van a ejecutar allí. Con esta información y aprovechando las herramientas disponibles en la compañía para gestión de identidades se configura la herramienta PAM (Privileged Access Management).

La elaboración de la matriz de roles y perfiles se realizó mediante validación al interior de la compañía para determinar los usuarios y las funciones que requieren ejecutar para el desarrollo de sus funciones acceder a los dispositivos de la red. Durante este proceso, se determinó que a los elementos OT solo deben tener acceso los ingenieros de seguridad quienes para el momento de la evaluación tenían privilegios de administrador. Por buenas prácticas este tipo de privilegios debería ser restringido, sin embargo, se concluye la necesidad de este perfil para lograr ejecutar las funciones en estos sistemas, no obstante, como parte de este mismo control se implementa un PAM que permitirá controlar los inicios de sesión en cada dispositivo, guardando un log de cada una de las acciones de forma individual.

La compañía cuenta con una solución de Gestión de acceso privilegiado PAM, (Privileged Access Management), una solución de seguridad de identidad que mediante la supervisión y detección de accesos ayuda a proteger las organizaciones contra materialización de incidentes de seguridad asociados al acceso con privilegios no autorizado a recursos críticos. PAM funciona mediante una combinación de procesos y tecnologías que ofrece visibilidad sobre quién está utilizando cuentas con privilegios y sus acciones mientras está conectado. Limitar el número de usuarios que tienen acceso a funciones administrativas incrementa la seguridad del sistema, mientras que las capas adicionales de protección mitigan la filtración de información llevada a cabo por actores de amenazas

B. Segundo control

Procedimiento de altas, bajas y modificaciones para la gestión de accesos – R5

El proceso de gestión de cuentas de usuario AMB Altas, Bajas y Modificaciones, es un control base que permitirá que a los sistemas solo tengan acceso las personas autorizadas, para lo cual requiere la definición e implementación de un procedimiento de altas, bajas y modificaciones de las identidades.

Cuando un colaborador requiere acceso a un sistema, ya sea por primera vez o debido a un cambio en sus responsabilidades, es necesario verificar su autorización y establecer los permisos correspondientes, este último detallado en el primer control implementado en el proyecto. De manera similar, cuando un colaborador deja la compañía, sus accesos deben ser revocados de manera oportuna para evitar posibles riesgos de seguridad.

El procedimiento de gestión de cuentas de usuario AMB propuesto también incluye la evaluación periódica de los accesos activos en los diferentes dispositivos. Esto garantiza que solo las personas autorizadas tengan acceso a la información y los recursos necesarios para desempeñar sus funciones. Se incluye el paso a paso para actualizar de forma regular de la matriz de roles y perfiles de tal forma que refleje los cambios en las responsabilidades y los requisitos de acceso de los colaboradores. Este enfoque garantiza que los controles de acceso estén alineados con las necesidades operativas y de seguridad de la organización.

C. Tercer control

Aseguramiento perimetral de la infraestructura – R1, R2, R5

El tercer control implementado es el aseguramiento perimetral de la infraestructura mediante la instalación y configuración de un firewall en la red. Este firewall, específicamente un dispositivo PA-440, se configura para garantizar la seguridad y el control de los equipos SCADA de la red de procesos, como servidores y PLCs. Esta medida busca minimizar la probabilidad de explotación de vulnerabilidades en

los equipos existentes de la red OT, protegiendo así el sistema contra posibles amenazas externas.

IV. GESTIÓN

A. Gobernanza

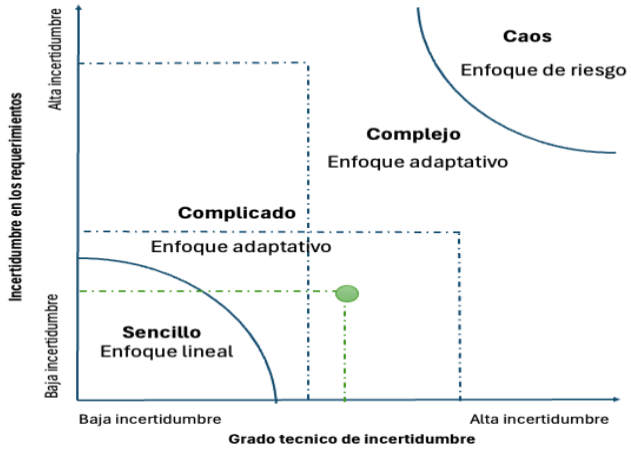
Tomando el planteamiento de Douglas Stancey, que cruza la "incertidumbre en los requerimientos" con el "grado técnico de incertidumbre", en donde sus valores van de un nivel bajo de incertidumbre a uno alto, es decir se cuenta con un grado de certeza alto que se puede predecir el resultado; hasta el punto opuesto no hay claridad de las causas o efectos por lo tanto la toma de decisiones es más riesgosa. (Palacios, 2021)

Dado lo anterior y considerando la información recadaba a la fecha de la compañía y el entorno relacionado a la implementación del proyecto se podría concluir la siguiente información en cada uno de los ejes del plano:

- **Incertidumbre en los requerimientos**: se considera una evaluación de baja incertidumbre pues se evidencia certeza en la inversión de recursos económicos, humanos y tecnológicos para implementación, esto considerando que la compañía esta impulsa este proyecto que le aporta a la seguridad de la información y proteger la operación de ciber ataques que puedan afectar la operación, los entornos naturales, así como impactos económicos y legales.

- **Grado técnico de incertidumbre:** para este caso el nivel de incertidumbre aumenta un poco, dado que la expertis y el manejo de la tecnología OT por parte del equipo de seguridad, requiere de trabajo adicional para su aprendizaje, por lo tanto, esto puede impactar en la consecución del proyecto.

Figura 6
Modelo de complejidad de Stacey



Nota: El modelo de complejidad permie identificar en el plano cual es mejor sugerencia para el tipo de enfoque que debe manejar el proyecto, en este caso es tipo complicado con enfoque adaptativo marcado en color verde. Fuente: Elaboración propia

Con lo anterior este proyecto se cataloga dentro del área de lo complicado pues requiere un planteamiento flexible que permita aprendizaje, con esto se plantea un tipo de enfoque adaptativo el cual se desarrolla con metodologías agiles. En la siguiente figura se puede observar gráficamente el resultado entre las dos variables identificadas.

B. Planteamiento ágil y cronograma

El proceso de desarrollo e implementación de estos controles se ha planificado en iteraciones de tres meses, que tomara un total de 21 meses, terminando la última iteración en noviembre de 2025. Durante cada iteración, se llevan a cabo los análisis necesarios para cada control y se implementan las acciones definidas. Es importante tener en cuenta que algunos controles pueden requerir más de una iteración debido a su complejidad, a las actividades cotidianas de los ingenieros y a la posible dependencia de terceros para su implementación. Este enfoque iterativo garantiza una implementación efectiva y una adaptación continua a los requisitos cambiantes de seguridad y operativos.

Figura 7
Cronograma de implementación de controles

Nota: Los controles a implementar se han asignado a una iteración en la que se consideraron los prerrequisitos. Fuente: Elaboración propia

La Figura 7 representa las iteraciones mediante las cuales se sugiere implementar los controles. Siendo en primer ciclo la puesta en producción de los 3 controles propuestos resultado del proyecto. Estas sugerencias se pueden adaptar a la evolución de la empresa considerando los cambios, el aumento del nivel de madurez de seguridad, nuevos recursos, entre otros que pueda presentar la compañía, aumentando o disminuyendo las iteraciones

V. CONCLUSIONES

La implementación del estándar ISA/IEC 62443-3-3, en los procesos operacionales de la organización, es una inversión estratégica con un retorno significativo en términos de seguridad, eficiencia, confiabilidad y confianza de los stakeholders. Si bien existen costos y desafíos asociados a la implementación, las ventajas a largo plazo son considerables y con seguridad generarán excelentes resultados.

La compañía actualmente tiene la preocupación de no contar con controles para mitigar los riesgos de la ciberseguridad

derivados de la interconexión entre las redes de tecnología de la información IT y tecnología operativa OT, que se establece con el objetivo de tomar decisiones estratégicas. Por esta razón alinearse con el estándar permitirá proteger la infraestructura crítica de la compañía contra ataques cibernéticos que podrían tener graves consecuencias, incluyendo la pérdida de datos confidenciales y la interrupción del servicio, lo que podría afectar significativamente las operaciones comerciales y la reputación de la empresa.

La falta de segmentación de red en la infraestructura SCADA de la compañía evaluada representa una seria deficiencia en la seguridad de la red. Esto se debe a que todos los dispositivos utilizan el mismo segmento de red, lo que facilita el movimiento lateral de un atacante una vez que ha obtenido acceso inicial. Esta falta de segmentación aumenta significativamente el riesgo de compromiso de la red y podría exponer la infraestructura crítica de la compañía a amenazas cibernéticas.

La ausencia de controles de seguridad, como el bloqueo de puertos no utilizados, la limitación de direcciones MAC autorizadas y la ausencia de herramientas centralizadas para restringir el ingreso operativo y administrativo en los switches de acceso de la infraestructura, así como la carencia de una infraestructura de monitoreo de fallos y detección de intrusiones, revela una falta de medidas preventivas y de respuesta ante posibles amenazas cibernéticas en la red SCADA. Este vacío en la seguridad expone la infraestructura crítica de la compañía a riesgos significativos y podría permitir a los atacantes comprometer la integridad y disponibilidad de los sistemas.

La inexistencia de lineamientos claros para el control de acceso, la segmentación de red y aplicación de parches de seguridad en la infraestructura crítica de la organización pone de manifiesto la falta de procedimientos y protocolos establecidos para salvaguardar la integridad y confidencialidad de los datos, así como para mitigar las vulnerabilidades y riesgos de seguridad en los sistemas operativos. Esta ausencia de directrices adecuadas aumenta la exposición de la organización a posibles amenazas cibernéticas y debilita su capacidad para proteger sus activos críticos contra intrusiones y ataques maliciosos.

Al establecer interconexión de redes de tecnología operativa OT e información IT, surge la necesidad imperativa de abordar un análisis de riesgos. Este análisis es crucial para comprender y abordar los desafíos de seguridad cibernética que conlleva dicha interconexión. Entre estos desafíos se incluyen la exposición a malware, vulnerabilidades en sistemas que no han sido diseñados para estar expuestos a internet y posibles consecuencias graves en las operaciones críticas de la organización. Es fundamental que la empresa identifique, evalúe y monitoree estos riesgos para implementar medidas efectivas de mitigación y protección de sus activos críticos frente a posibles amenazas cibernéticas.

Para mitigar los riesgos identificados, es fundamental implementar medidas como la segmentación de redes, controles de acceso estrictos y la monitorización continua de la actividad de la red. Además, la colaboración y comunicación efectivas entre los equipos de OT y IT y transferir riesgos a proveedores especializados de SOC son esenciales para garantizar una respuesta rápida y eficaz a posibles incidentes de seguridad.

La norma ISA 62443-3-3 proporciona diferentes niveles de seguridad que pueden ser implementados y mantenidos en los sistemas de OT. Sus controles deben evaluarse y adaptarse a las necesidades puntuales y características de cada compañía con el objetivo de robustecer la seguridad.

Aunque la compañía cuenta con herramientas utilizadas actualmente en la red de tecnología de la información IT que pueden ser adaptadas y aprovechadas para el trabajo en las redes de tecnología operativa OT. en algunos casos, también puede ser necesario tercerizar tareas específicas para garantizar un despliegue efectivo de las soluciones de seguridad en la tecnología operativa OT.

La implementación del estándar ISA/IEC 62443-3-3, ofrece una guía muy completa para mejorar la protección contra las amenazas cibernéticas, de la compañía, sin embargo, es recomendable concientizar al personal sobre la importancia de la seguridad cibernética y fomentar un comportamiento responsable.

VI. Trabajo futuro

La empresa debe continuar con la implementación de los controles definidos y evaluados, los cuales contribuirán a prevenir la materialización de riesgos y reducir su impacto y probabilidad en caso de que ocurran. Estos controles se han planificado con ciclos de 3 meses que iniciaron con el desarrollo de este proyecto y terminando en noviembre de 2025, durante los cuales se implementan controles en un orden definido, considerando los prerrequisitos y la disponibilidad de recursos humanos. Es importante tener en cuenta que el proyecto cuenta con los recursos económicos presupuestados necesarios para adquirir herramientas, licencias y servicios que garanticen el éxito de esta implementación.

Se recomienda tomar medidas inmediatas para proteger los activos críticos existentes y minimizar el riesgo de un ataque cibernético. Esto realizando la implementación de los controles presentados en el proyecto que parten de las medidas básicas de seguridad y progresivamente asegurando los niveles en la red SCADA, abordando cada uno de los aspectos de vulnerabilidad identificados de manera gradual y sistemática.

Es claro a su vez que, se requiere la implementación urgente de una estrategia de segmentación de red en la infraestructura SCADA. Separar los segmentos de red de los PLC y servidores es fundamental para reducir la superficie de ataque y limitar el movimiento lateral de posibles amenazas cibernéticas. Esto ayudará a fortalecer la seguridad de la red y proteger los activos críticos de la organización.

Por otro lado, es necesario establecer controles de seguridad aterrizados a las necesidades de la compañía en los switches de acceso de la infraestructura. Esto incluye el bloqueo de puertos libres, limitación de direcciones MAC autorizadas y la implementación de herramientas centralizadas para restringir

accesos, con el fin de fortalecer la protección de la red SCADA y prevenir posibles intrusiones o ataques cibernéticos.

Así mismo, se infiere la importancia de desarrollar e implementar un plan integral de gestión de parches de seguridad que incluya la identificación y evaluación proactiva de vulnerabilidades, el despliegue seguro de parches, la verificación de su efectividad y la comunicación de riesgos asociados a la explotación de vulnerabilidades. Estas medidas contribuirán a mantener actualizados los sistemas operativos críticos y a reducir la exposición a posibles amenazas de seguridad.

Es fundamental que la organización reconozca y ejecute análisis de riesgos a todos los proyectos que involucren redes OT, dado que están manejan operaciones que se consideran CORE de la compañía. Dejar expuesta la operación y la información puede implicar desde impactos económicos hasta legales y de vidas, entre otros, que pueden ser identificados y mitigados con una correcta gestión de riesgos.

Ahora bien, teniendo en cuenta la mejora continua que deben tener los controles de seguridad para garantizar que su diseño y ejecución se mantiene fuerte durante el tiempo, se requiere realizar una evaluación periódica a los riesgos y ejecución de los controles, al menos una vez al año. Esta evaluación debe incluir un análisis con evidencia de la ejecución de cada uno de los controles establecidos, lo que permita validar que se han estado ejecutando y de esta forma garantizar que se mantenga el nivel de riesgo residual dentro del apetito de riesgo. Además, esta evaluación ayudará a identificar nuevos riesgos derivados de cambios en la tecnología y la operación, y contribuirán a aumentar el nivel de madurez de seguridad de la compañía.

VII. Referencias

[1] ANSI/ISA-62443-1-1 (99.01.01), Security for industrial automation and control Systems: Part 1-1, Terminology, concepts and models3

[2] ANSI/ISA-62443-2-1 (99.02.01), Security for industrial automation and control systems: Part 2-1, Requirements for an IACS security management systemZ

[3] Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. Public Administration Review, 81(5), 847-861. https://doi.org/10.1111/puar.13322

[4] Cerqueira Junior, A. S., & Arima, C. H. (2023). Cyber Risk Management and Iso 27005 Applied in Organizations: A Systematic Literature Review. REVISTA FOCO, 16(02), e1188. https://doi.org/10.54751/revistafoco.v16n2-215

[5] G. Eason, B. Noble, and I.N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” *Phil. Trans. Roy. Soc. London*, vol. A247, pp. 529-551, April 1955.

[6] García, M. T. M. (2022). Gestión de incidentes de ciberseguridad. RA-MA S.A. Editorial y Publicaciones.

[7] ICONTEC NTC ISO/IEC 27005:2008 Tecnología de la Información – Técnicas de Seguridad – Gestión del riesgo de seguridad de la información

[8] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism*, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[9] NBR ISO/IEC 27005 – Tecnología da información – Técnicas de seguridad– Gestión de riscos de seguridad de la información.

[10] Palacios, J. (2021). Entendiendo la complejidad: La matriz de Stacey. Recuperado 5 de Marzo de https://academy.jeronimopalacios.com/courses/145560/lectures/5315213