Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

MAESTRÍA EN CIBERDEFNSA Y CIBERSEGRIDAD

PROYECTO

TRABAJO FINAL DE MAESTRÍA

Gestión de vulnerabilidades en sistemas de control industrial

Vulnerability management in industrial control systems

AUTOR: MATIAS FEDERICO MANASSERO

DIRECTOR: MARISA ANDREA MALVASO

Mayo 2023

Esta página ha sido dejada en blanco intencionalmente

i. Resumen del Proyecto

La interconexión creciente entre los mundos de OT (tecnología operativa) y de IT (tecnología de la información) ha generado la necesidad de desarrollar prácticas específicas de ciberseguridad para entornos industriales. La tesis de maestría se enfoca en la gestión de vulnerabilidades en sistemas de control industrial de automatización (AICS)[1], un subconjunto de las vulnerabilidades de ciberseguridad en la industria 4.0[2]. La interconexión entre redes operativas, incluyendo aquellas con diferentes niveles de seguridad, ha aumentado la exposición a amenazas cibernéticas en entornos industriales, lo que hace esencial la gestión adecuada de vulnerabilidades.

La gestión de vulnerabilidades en una red industrial es crucial para mantener la disponibilidad del entorno, pero es difícil debido a la necesidad de operación continua y la inexistencia de posibles correcciones. Por lo tanto, esta investigación propone procesos, procedimientos y mejores prácticas para la gestión de vulnerabilidades en entornos industriales con el objetivo general de definir el proceso de gestión de vulnerabilidades para la mitigación de riesgos en sistemas de entornos industriales.

En entornos industriales, la continuidad del proceso productivo es prioritaria, y a menudo se da prioridad a la disponibilidad sobre la integridad y confidencialidad de la información. Para garantizar tanto la protección de la información crítica como la continuidad del proceso productivo, es fundamental diseñar medidas de seguridad específicas para estos entornos. La implementación de medidas de protección adecuadas y efectivas es respaldada por el marco internacional de ciberseguridad industrial ISA-62443.

Palabras claves: OT (tecnología operativa), IT (tecnología de la información), Vulnerabilidades, Control industrial de automatización (AICS), Industria 4.0, Redes operativas, Amenazas cibernéticas, Gestión de vulnerabilidades, Procesos, Procedimientos, Mitigación de riesgos, Marco internacional de ciberseguridad industrial.

[1] Industrial Automation and Control System.

[2] El concepto de Industria 4.0 refiere a una nueva manera de producir mediante la adopción de tecnologías 4.0, es decir, de soluciones enfocadas en la interconectividad, la automatización y los datos en tiempo real (*¿Qué Es La Industria 4.0? | Argentina.Gob.Ar*, n.d.)

ii. Abstract

The growing interconnection between the worlds of OT (operational technology) and IT (information technology) has created the need to develop specific cybersecurity practices for industrial environments. This master's thesis focuses on vulnerability management in industrial control systems of automation (AICS), a subset of cybersecurity vulnerabilities in industry 4.0. The interconnection between operational networks, including those with different security levels, has increased exposure to cyber threats in industrial environments, making proper vulnerability management essential.

Managing vulnerabilities in an industrial network is crucial to maintain the availability of the environment, but it is challenging due to the need for continuous operation and the lack of possible corrections. Therefore, this research proposes processes, procedures, and best practices for vulnerability management in industrial environments with the general objective of defining the vulnerability management process for risk mitigation in industrial environments.

In industrial environments, process continuity is prioritized, and availability is often given precedence over information integrity and confidentiality. To ensure the protection of critical information and process continuity, it is essential to design specific security measures for these environments. The implementation of adequate and effective protection measures is supported by the international framework for industrial cybersecurity, ISA-62443.

Keywords: OT (operational technology), IT (information technology), Vulnerabilities, Industrial automation control system (IACS), Industry 4.0, Operational networks, Cyber threats, Vulnerability management, Processes, Procedures, Risk mitigation, Process continuity, Critical information, International industrial cybersecurity framework (ISA-62443).

Esta página ha sido dejada en blanco intencionalmente.

iii. Dedicatorias

Quiero dedicar esta tesis a las personas más importantes en mi vida: en primer lugar, a mi novia, quien ha sido mi compañera en todo momento, brindándome su apoyo incondicional y motivándome a seguir adelante en los momentos más difíciles.

También quiero expresar mi gratitud hacia mis padres, quienes me han enseñado los valores que me han guiado en esta etapa de mi vida, y quienes me han dado la educación y las oportunidades que me han permitido llegar hasta aquí. A ambos, les dedico este logro como un homenaje a su amor y dedicación hacia mí.

iv. Agradecimientos

A mi excepcional Directora de Tesis, la Esp. Lic. Marisa Andrea Malvaso, por ser mi guía, apoyo, líder y mentora durante todo este proceso. Su dedicación y conocimiento me permitieron alcanzar este logro académico. Agradezco su amistad y compromiso incondicional en mi crecimiento personal y profesional.

Agradezco de manera especial al Dr. Roberto Uzal y al Ing. Carlos Amaya por su dedicación y compromiso en la creación y desarrollo de esta Maestría en Ciberdefensa y Ciberseguridad. Gracias a su incansable trabajo, tuve la oportunidad de adquirir los conocimientos y habilidades necesarios para crecer tanto profesional como personalmente.

Agradezco a mis hermanos, amigos, colegas y a todas las personas que directa o indirectamente me acompañaron en esta etapa. Su apoyo fue fundamental para alcanzar la finalización de este proyecto.

Esta página ha sido dejada en blanco intencionalmente

Índice

Índice general

Índice de tablas

Índice de figuras

Justificación

En el pasado, las tecnologías de la información (IT)[3] y las tecnologías de operación (OT)[4] se encontraban en ambientes aislados entre sí. Esto se debía en gran parte a que los sistemas industriales se basaban principalmente en plataformas propietarias de SCADA (General Electric, Rockwell, Schneider, Siemens, entre otros), mientras que los sistemas IT utilizaban hardware genérico y sistemas operativos que podían ser propietarios o de código abierto.

La evolución de las tecnologías tuvo como resultado la convergencia entre el mundo IT y el mundo OT, lo cual permitió potenciar sus funcionalidades, teniendo en cuenta que tienen objetivos diferentes y que los entornos sobre los cuales trabajan cada uno de los entornos también difieren. Conocer estas diferencias entre ambos mundos permite asegurar una convergencia responsable y funcional en el sector de la Industria 4.0.

En entornos de operaciones (OT), la prioridad principal es mantener la continuidad del proceso industrial y la seguridad de las personas, lo que deriva en que la experiencia de usuario se sitúe en un segundo plano. Sin embargo, una mala experiencia de usuario en OT puede tener consecuencias graves, como errores humanos, accidentes o fallos en el proceso. Por tanto, es importante que se preste atención a la experiencia de usuario en OT y se diseñen soluciones que permitan un equilibrio entre la seguridad y la eficiencia operativa, así como una formación adecuada y un diseño de interfaces intuitivo y fácil de usar (International Society of Automation, 2017).

Por este motivo, es que se realiza una investigación sobre cuáles son los riesgos de una infraestructura vulnerable y qué contramedidas se pueden aplicar para disminuir el impacto y la probabilidad de explotación de las vulnerabilidades. A tal fin el propósito de la investigación es la gestión de vulnerabilidades en entornos industriales para mitigar los riesgos.

[3] Information Technology.
[4] Operational Technology.

Planteamiento del problema

Existen diversas normativas[5] específicas en el ámbito de OT, adaptadas a cada sector industrial en particular debido a las diferencias entre los procesos industriales. Por tanto, es difícil encontrar normativas generalistas que abarquen todos los aspectos de las operaciones[6].

Es importante tener en cuenta que en los entornos de operaciones industriales, la prioridad principal es mantener la continuidad del proceso productivo, lo que puede llevar a que se dé prioridad a la disponibilidad por encima de la integridad y confidencialidad de la información. Además, en estos entornos es común que los usuarios tengan una experiencia limitada en términos de seguridad informática y que se enfocan más en el uso de los sistemas que en su protección. Por tanto, es fundamental diseñar medidas de seguridad adaptadas a estos entornos para garantizar la protección de la información crítica y la continuidad del proceso productivo.

Es por este motivo, que la ciberseguridad industrial está alineada a los objetivos de la operación en cuanto a la continuidad del proceso industrial sin perder el foco en todas las capas que componen la seguridad.

A fin de sustentar la investigación en un marco de ciberseguridad basado en estándares internacionales y guiado por muchas perspectivas (sector privado, académico, público) se fundamenta este trabajo alineándose con el marco internacional de ciberseguridad industrial (ISA-62443)[7], que permite, no solo enmarcar la investigación, sino también fundamentar, a través de las referencias informativas específicas, el desarrollo y la implementación apropiada de contramedidas para asegurar la entrega de servicios por parte de los procesos.

[5] ISA/IEC 62443, NERC-CIP.

[6] El NIST CSF es un marco de trabajo de ciberseguridad que se puede alinear con otros estándares de referencia, tales como el NERC o la ISA, lo que permite una mayor integración con los objetivos y requisitos regulatorios de la organización.

[7] https://www.isa.org/

Hace unos años, este apartado no habría sido tan relevante como lo es en la actualidad. Como se menciona en la introducción, la inclusión de tecnologías comerciales fuera de la estandarización de la industria (COTS, por sus siglas en inglés) (International Society of Automation, 2020) aumenta las amenazas en la red industrial, al igual que la conexión entre redes de OT y de IT. Anteriormente, el vector de ataque era menor y la explotación de vulnerabilidades era principalmente local. Sin embargo, con la llegada de la Industria 4.0 y la interconexión de ambos mundos, este paradigma ha cambiado.

La interconexión de ambos entornos ha brindado numerosas ventajas, sin embargo, también ha aumentado significativamente la probabilidad de que un agente malintencionado aproveche las vulnerabilidades existentes a través del nuevo vector de ataque generado como consecuencia de la interconexión.

En la actualidad, la interconexión entre los mundos IT y OT es inviable debido a la importancia de la captura de datos en tiempo real en la toma de decisiones en la producción industrial. La obtención de información valiosa a nivel de negocio a través de los datos en tiempo real se ha convertido en una ventaja competitiva para las empresas. Por tanto, es necesario pensar en nuevos paradigmas de diseño de arquitecturas seguras que permitan prevenir ataques y responder de manera rápida ante cualquier amenaza en los entornos industriales interconectados.

Para que una arquitectura sea segura, se deben abordar diferentes puntos estratégicos, siendo la gestión de vulnerabilidades de entornos industriales, específicamente las vulnerabilidades de software/firmaware dentro de la red industrial uno de los puntos a desarrollar en este trabajo. Por tanto, es necesario entender: ¿Qué es la evaluación y gestión de vulnerabilidades de sistemas?

Por otro lado, la normativa ISA 62-443 publicó un informe interno en el cual define la gestión de vulnerabilidades como: "*Fallo o debilidad en el diseño, la implementación o el funcionamiento y la gestión de un sistema que podría ser explotado para dañar la integridad o la política de seguridad del sistema"* (International Society of Automation, 2017).

Las características de estos equipos de OT plantean la necesidad de un enfoque diferente: no intrusivo, con inspección de protocolos específicos de control industrial, y con detección de vulnerabilidades propias del tipo de elemento involucrados (PLCs, RTUs, sensores, estaciones de control SCADA, estaciones de ingeniería, etc.)

Para lograr una adecuada gestión de vulnerabilidades en entornos industriales, es fundamental comprender el proceso para identificar y mitigar estas vulnerabilidades con la adecuada priorización. Se considera indispensable contar con un inventario de activos que permita asociar las vulnerabilidades con las versiones de software de los equipos de campo, así como la planificación de las ventanas de aplicación para la mitigación. Además, se debe tener en cuenta que el proceso de gestión de vulnerabilidades debe ser cuidadosamente planificado para evitar interrupciones en el proceso industrial.

La problemática abordada en este trabajo se enfoca en la gestión de vulnerabilidades de software en entornos industriales, ya que las consecuencias de una falla en estos sistemas pueden tener un impacto significativo en la continuidad del proceso industrial. Es importante destacar que el tratamiento de estas vulnerabilidades es diferente al que se utiliza en entornos IT, por lo que se requiere de un enfoque específico para mitigar adecuadamente los riesgos en este tipo de entornos de red.

Objetivos

Objetivo General

- Definir el proceso de gestión de vulnerabilidades en los sistemas de entornos industriales para la mitigación de riesgos.

Objetivos Específicos

- Explorar el estado del arte en cuanto a procesos , metodologías y estándares para la gestión de vulnerabilidades de software en entornos industriales, identificando potenciales oportunidades de mejora.
- Estudiar y establecer las pautas mínimas e indispensables que se deben tener en cuenta para el proceso de gestión de vulnerabilidades de manera tal de no impactar el proceso industrial.
- Proponer potenciales procesos para la mitigación de las vulnerabilidades de software en sistemas industriales que disminuyan el riesgo de interrumpir la continuidad del proceso industrial.

Hipótesis

La gestión de vulnerabilidades de sistemas en entornos industriales requiere un proceso bien definido para disminuir el impacto de la aplicación de contramedidas en la continuidad del proceso industrial.

Hipótesis secundaria

No existe una metodología específica establecida formalmente para la gestión de vulnerabilidades en entornos industriales.

Marco Teórico

La gestión de vulnerabilidades en entornos industriales ha adquirido un papel fundamental en las empresas que buscan proteger sus activos y asegurar la continuidad de sus operaciones. En un mundo donde las amenazas cibernéticas están en constante evolución y cada vez son más sofisticadas, la identificación y gestión de vulnerabilidades se convierte en una tarea esencial para minimizar los riesgos tecnológicos que pueden afectar la seguridad de los activos críticos.

En este entorno en constante cambio y evolución continua de las amenazas, las empresas invierten recursos y esfuerzos para mantener los riesgos en un nivel tolerable previamente establecido en la organización. De esta forma, se busca maximizar los beneficios de la gestión sin perder de vista el objetivo general.

En este contexto, la presente tesis de maestría tiene como objetivo profundizar en la gestión de vulnerabilidades industriales, evaluando los diferentes enfoques y estrategias utilizados en la industria para abordar esta problemática, por lo cual se introduce el tema dentro del marco del proceso de evaluación de riesgos que toda organización debería llevar a cabo, siendo que, el concepto fundamental en una evaluación de riesgos, es la probabilidad de que una amenaza explote una vulnerabilidad y las consecuencias (impacto) que se pueden producir al manifestarse sobre los activos.

Proceso de Evaluación de riesgos

Para una correcta evaluación de riesgos, es importante la elección de una metodología que guíe la actividad y permita llevarla a cabo de manera sólida y estandarizada.

Como elemento fundamental de toda metodología de evaluación de riesgos, el inventario de activos es una pieza clave, ya que el resultado depende del conocimiento de los activos, de las relaciones que tengan entre sí, y también de las dependencias que existan entre ellos.

La organización debe establecer el umbral del riesgo para no superar el nivel máximo definido que puede soportar, por lo que a través de una adecuada gestión de riesgos se trabaja para mantener el nivel por debajo del umbral definido.

Para mantener este umbral se debe contar con recursos y esfuerzos dedicados, los cuales van a tener un costo para la organización, denominados costo de producción (Incibe - Instituto Nacional de Ciberseguridad, 2015).

La siguiente figura presenta una visión del proceso de gestión de riesgos tecnológicos de acuerdo con la norma ICONTEC NTC-ISO/IEC 27005:

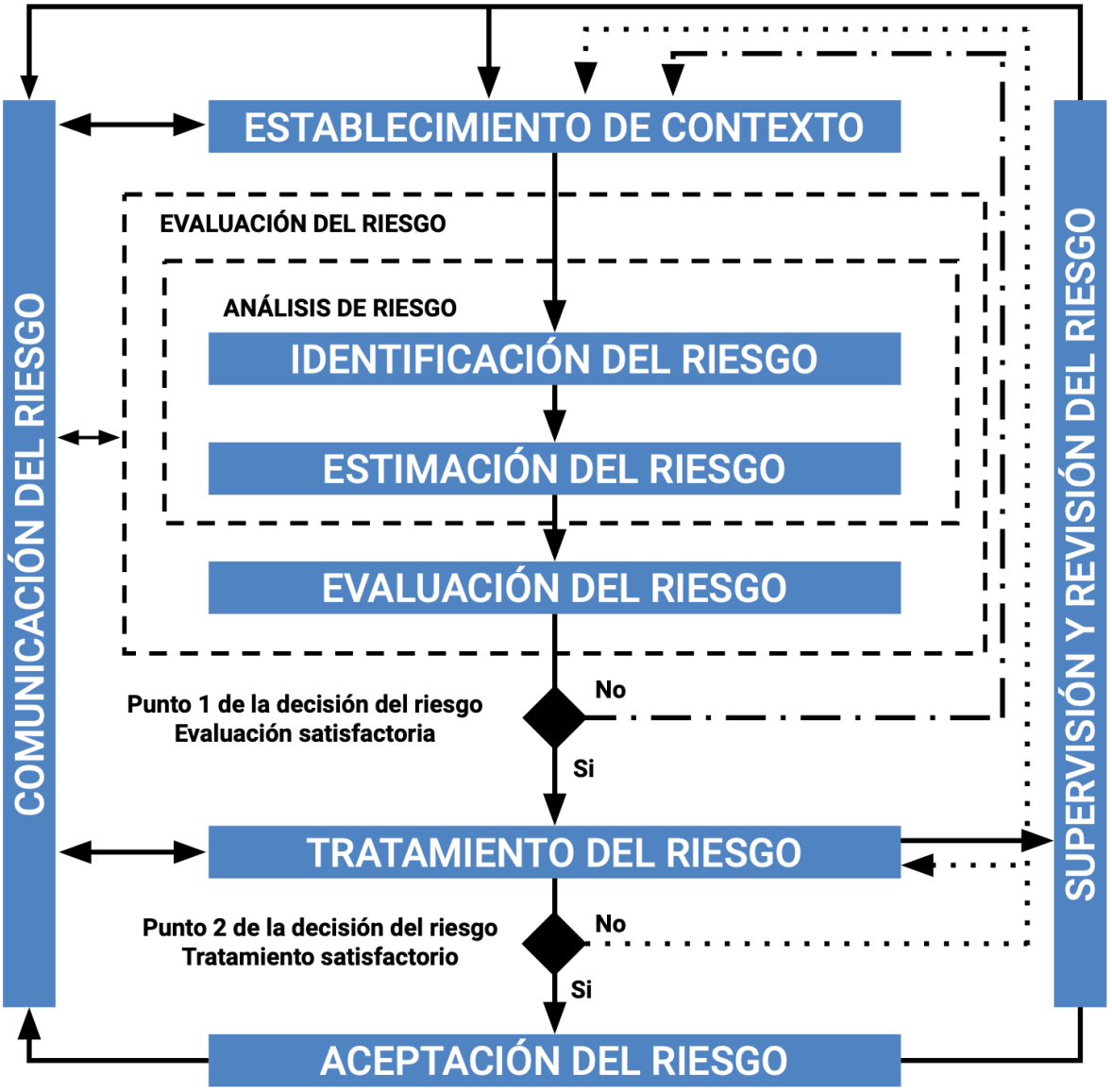

Figura 1- Proceso de gestión de riesgos (Dirección Nacional - Interoperabilidad, 2020)

El proceso consta de seis grandes grupos de actividades:

- **Establecimiento del contexto:** La definición de contexto es responsable de definir el ambiente, alcance, criterios de evaluación, y otros ajustes. Esta etapa es esencial para el equipo que lleva a cabo la gestión del riesgo de conocer toda la información sobre la organización.
- **Análisis/Evaluación del riesgo:** Permite la identificación del riesgo y la determinación de las acciones necesarias para reducir el riesgo a un nivel aceptable.
- **Tratamiento del riesgo:** Incluyen los controles necesarios para el tratamiento del riesgo, los cuales se definen a partir de los resultados obtenidos del análisis y la evaluación del riesgo. Las distintas normativas sugieren diversas medidas y controles que deben ser implementados.
- **Aceptación del riesgo:** Documentar los riesgos que la organización está dispuesta a asumir, lo cual se logra mediante un análisis y justificación adecuados. En general, estos riesgos son aquellos cuyo costo de mitigación es mayor que el costo de asumirlos, o aquellos que tienen limitaciones en la aplicación de las contramedidas adecuadas.
- **Comunicación del riesgo:** Durante esta fase, se realiza la comunicación del riesgo y su correspondiente tratamiento a todas las partes interesadas, tanto internas como externas, abarcando las áreas operativas y sus respectivos equipos de gestión.
- **Supervisión y revisión del riesgo:** Son las actividades de acompañamiento de los resultados, implementación de controles y análisis crítico para la mejor continua del proceso de gestión del riesgo.

Además de las actividades mencionadas anteriormente, se destacan los siguientes tres pasos principales que integran el proceso: Identificación, Análisis y Evaluación concretamente dicha:

- **Identificación del riesgo:** En este punto se determinan los eventos que pueden causar potenciales pérdidas.
- **Análisis del riesgo:** En este punto se determina la probabilidad de ocurrencia de los eventos.

- **Evaluación del riesgo:** En este punto se ordenan los riesgos de acuerdo con los criterios de evaluación establecidos en la definición de contexto.

Identificación del riesgo

En el proceso de evaluación del riesgo, el primer paso es la identificación del riesgo. Esta fase busca determinar los posibles eventos que pueden causar pérdida o algún impacto en la organización.

Las organizaciones deben identificar sus riesgos, causas y consecuencias debido a que esto les permite generar un listado de los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos.

Las actividades de identificación de riesgos se muestran a continuación en la siguiente figura:

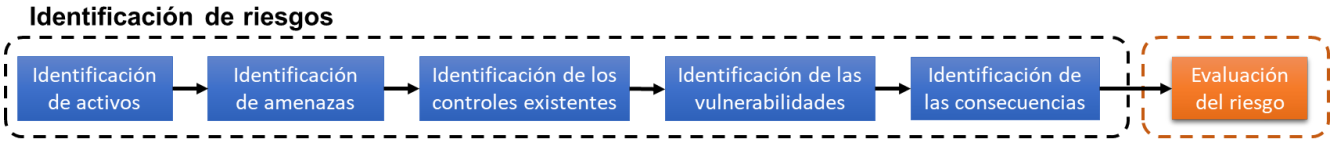

Figura 2 - Actividades de identificación del riesgo (Kowask Bezerra et al., 2021)

A continuación se detallan cada una de estas actividades, con el objetivo de profundizar en el enfoque de esta tesis que es la gestión de vulnerabilidades.

1. Identificación de activos

La fase de identificación de activos es un componente importante en la gestión de vulnerabilidades de la organización. En esta etapa, se busca identificar todos aquellos activos que son de valor para la organización y, por ende, requieren protección. Los activos pueden ser tanto físicos como virtuales, y pueden incluir hardware, software, datos, redes, instalaciones, entre otros.

El objetivo de la identificación de activos es obtener una comprensión clara y precisa de los activos que se deben proteger y su relación con otros activos de la organización. De esta forma, se pueden determinar las amenazas y vulnerabilidades a las que están expuestos, y el nivel de riesgo o exposición de cada uno de ellos.

Para llevar a cabo esta identificación, se deben seguir diversas etapas. En primer lugar, se deben contemplar los resultados de la definición del alcance para determinar el listado de activos que son alcanzados por la gestión de riesgo. Luego, se procede a la identificación de los activos, lo cual se puede hacer de manera manual o automática a través de herramientas especializadas de descubrimiento. Es importante que el nivel de detalle en la identificación permita suministrar información adecuada y suficiente para el análisis y evaluación del riesgo.

La salida de esta etapa es una lista de los activos considerados sensibles para la organización, así como una lista de los procesos relacionados a estos activos. La información obtenida en esta etapa servirá como base para la evaluación de vulnerabilidades y la definición de las contramedidas necesarias para mitigar los riesgos identificados.

2. Identificación de amenazas

La actividad de identificación de amenazas será realizada a través de acciones que permitan encontrar, dentro del alcance establecido, las amenazas existentes en la organización.

De esta actividad de identificación de las amenazas se obtendrá lo siguiente (Kowask Bezerra et al., 2021).

- **Entrada**: La identificación de amenazas para la gestión de riesgos se puede basar en la información de su historial, obtenida a partir de incidentes ocurridos y observaciones realizadas por los responsables y usuarios de los activos, así como de catálogos externos de amenazas. Sin embargo, con la creciente sofisticación de los ataques informáticos, puede que no siempre exista un historial de amenazas. En estos casos, puede ser necesario recurrir a técnicas avanzadas de análisis de

comportamiento para identificar riesgos y amenazas potenciales. De esta manera, se indica que la identificación de riesgos puede basarse en el historial de amenazas, pero se menciona que en la actualidad puede que no siempre exista esta información y se ofrecen alternativas para abordar esta situación.

- **Acción**: Identificación de las amenazas y sus fuentes. La fuente de amenaza está relacionada a su agente, entidad que puede causar una amenaza explotando o evidenciando alguna vulnerabilidad. Uno de los principales y más peligrosos agentes de amenaza es el ser humano.
- **Salida**: Lista de amenazas con la identificación del tipo y de la fuente de las amenazas.

En el proceso de identificación de amenazas es necesaria la creación de un catálogo de amenazas de la organización que incluya, entre otras características, como podría ser la frecuencia de ocurrencia en el contexto y el origen de la amenaza:

- Interna (origen dentro de la organización)
- Externa (origen fuera de la organización)
- Interna y externa simultáneamente.

3. Identificación de los controles (contramedidas) existentes

En este trabajo se utilizarán indistintamente los términos "controles", "contramedidas" o "salvaguardas" para hacer referencia a las medidas de seguridad implementadas con el fin de proteger los activos de la organización contra posibles amenazas y vulnerabilidades.

Es importante realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles, este proceso se suele conocer como **racionalización de controles**. Además, mientras se identifican los controles existentes se deben verificar para garantizar que los controles funcionan correctamente. Si el control no funciona como se espera, puede causar vulnerabilidades (verificar la eficiencia y eficacia de los controles implementados).

El objetivo es identificar en el ambiente el alcance de los controles definidos para implementar, los controles existentes y cuáles de ellos actualmente están en uso:

- **Entrada**: Documentación de los controles ya existentes y los planes de implementación de controles para el tratamiento del riesgo.
- **Acción**: Identificación de los controles implementados y planificados.
- **Salida**: Lista de todos los controles existentes y planeados, su implementación y estado de uso (eficacia y eficiencia).

En esta etapa se debe evaluar si es necesario agregar controles complementarios para el tratamiento eficaz del riesgo o remover y/o reemplazar los controles que son ineficaces o insuficientes.

4. Identificación de las vulnerabilidades

En la secuencia de este proceso, como se mencionó en los apartados anteriores, después del conocimiento del contexto del ambiente en el que se realizará la evaluación del riesgo, se identifican los activos, las amenazas, los controles existentes y también aquellos que necesitan ser implementados. El siguiente paso consiste en identificar las vulnerabilidades y las consecuencias que pueden ser causadas en caso de que las vulnerabilidades sean explotadas.

La actividad de identificación de las vulnerabilidades tiene como objetivo crear una lista con las vulnerabilidades asociadas a los activos, amenazas y controles. En esta actividad, el equipo de análisis tendrá como:

- **Entrada**: listas de amenazas conocidas, listas de los activos y de los controles existentes, y todas las salidas de las actividades anteriores (Identificación de activos, Identificación de amenazas, Identificación de los controles existentes).
- **Acción**: actividad de identificación de las vulnerabilidades que podrían ser explotadas por amenazas con la posibilidad de poner en peligro los activos.
- **Salida**: lista de escenarios de incidentes con sus consecuencias asociadas con los activos y los procesos de negocio.

Las vulnerabilidades podrían clasificarse en dos grandes grupos (Romero et al., 2018), los cuales se mencionan a continuación:

- Vulnerabilidades físicas.
- Vulnerabilidades lógicas.

4.1.Vulnerabilidades físicas

Las vulnerabilidades físicas son aquellas que afectan la infraestructura de la organización de manera física. Ejemplos de este tipo de vulnerabilidades son los desastres naturales, como los terremotos o inundaciones que pueden interrumpir el servicio y afectar la disponibilidad. Otra forma de vulnerabilidad física son los controles de acceso físicos deficientes que permiten que cualquier persona tenga acceso a la infraestructura crítica. Esto aumenta el riesgo de que un usuario malintencionado pueda ingresar con una unidad USB y copiar información o infectar la infraestructura. Es importante que las organizaciones identifiquen y mitiguen estas vulnerabilidades físicas para proteger su infraestructura crítica y garantizar la continuidad del negocio (Romero et al., 2018).

4.2.Vulnerabilidades lógicas

La protección de los sistemas de información y la información que manejan depende en gran medida de las vulnerabilidades intrínsecas de los activos en cuestión. Tales vulnerabilidades pueden variar según la naturaleza de los sistemas, abarcando aspectos como el hardware, el software, las redes, el personal, las instalaciones y la organización en sí misma. Por tanto, es importante identificar y mitigar estas vulnerabilidades para garantizar la seguridad y la continuidad de los procesos de la organización.

Desde la perspectiva de la gestión de riesgos, las vulnerabilidades pueden clasificarse en cuatro categorías:

Vulnerabilidades de gestión

Las vulnerabilidades de gestión se definen como fallos o insuficiencias en los procesos, políticas y prácticas de gestión de una organización que pueden facilitar la explotación de una amenaza o incidente de seguridad.

Presupuestos Ad hoc: La seguridad se debe enfocar como un programa a seguir de forma continua y no como un ejercicio puntual, ya que hay que estar continuamente adaptándose al ritmo al cual avanza. Una solución de seguridad que no se adapte a las amenazas existentes no cumplirá con los objetivos para la cual ha sido diseñada.

Formación: Debido a que cada día aparecen nuevas vulnerabilidades, un aspecto crítico que se debe tener en cuenta es la formación del personal que gestiona cualquier ámbito de la seguridad.

Vulnerabilidades operacionales

Las vulnerabilidades operacionales se refieren a debilidades en los procesos, procedimientos y controles operativos de una organización que pueden permitir la explotación de una amenaza o incidente de seguridad.

Segmentación de red: Muchas organizaciones tienen la red industrial como una extensión de la red IT debido a la necesidad de acceder a los datos en cualquier momento. Es recomendable separar el tráfico de ambas redes.

Gestión de cuentas: En redes industriales, con frecuencia, la eficiencia administrativa implica una carencia en prácticas de seguridad. Por ejemplo, compartir la cuenta de administrador o tener contraseñas comunes a varios usuarios suele ser una práctica común.

Procedimientos de acceso remoto: Controlar el acceso, las cuentas de usuario utilizadas, las direcciones IP que pueden acceder, los permisos, auditar la seguridad del proveedor que se conecta y restringir el acceso por zonas entre otros es una tarea obligatoria.

Despliegue de sistemas Wireless: El acceso a estas redes es mucho más fácil que a una red física. Son mucho más fáciles de detectar y suelen tener una arquitectura de seguridad menos robusta.

Procedimiento de detección de incidentes: En la gran mayoría de casos no existe un procedimiento específico para detectar amenazas. Aunque un sistema comprometido es difícil de diagnosticar, es posible basarse en otro tipo de indicadores que muestran un funcionamiento anómalo del sistema, como puede ser el uso excesivo de recursos del sistema o picos en el uso de red.

Gestión del cambio: Una gestión del cambio inexistente o no rigurosa representa un alto riesgo. Una gestión del cambio pobre en el entorno IT es otra vulnerabilidad para una red industrial. Por ejemplo: una modificación en la configuración de un switch u otra electrónica que se comparta con la red industrial o un switch dedicado para nuestra red gestionado por IT debido a su fragilidad.

Vulnerabilidades funcionales

Las vulnerabilidades funcionales se refieren a las debilidades en los procesos y procedimientos en la organización que pueden ser explotados por un atacante para acceder, dañar o comprometer sistemas y activos.

Conexión de redes a través de dispositivos: Los dispositivos de campo suelen estar formados por dos interfaces, una conectada a la red IP desde la cual le llegan órdenes de un servidor SCADA, y la interfaz de E/S, la cual controla las funciones físicas de producción.

Denegación de visión y pérdida de visión: Resultado de un fallo temporal o permanente de las comunicaciones en la tarjeta IP. La afectación funcional es la pérdida de la información en el proceso de producción.

Manipulación de visión: Modificación de los datos que el operador visualiza para provocar una acción inapropiada. En este caso no hay impacto en la funcionalidad de la interfaz IP o la de IO.

Denegación de control y pérdida de control: Denegación temporal o permanente del control sobre la interfaz de E/S.

Manipulación de control: Intercepta las funciones que envía el operador al dispositivo para modificar el código causando reacciones que afecten al proceso de producción.

Vulnerabilidades técnicas

La lista de vulnerabilidades relacionadas con software, hardware o la red es extensa y en constante crecimiento, lo que hace difícil mantenerla actualizada.

La cantidad de fallos que se publican diariamente hace que resulte prácticamente imposible elaborar una lista completa y exhaustiva.

Sistemas sin actualizar: Debido al ciclo de vida de los sistemas de control, muchos sistemas ejecutan firmwares y sistemas operativos sin actualizar, los cuales tienen vulnerabilidades. La gran mayoría de sistemas de control utilizan los mismos sistemas operativos que un departamento IT con las mismas vulnerabilidades, pero sin el mismo nivel de parcheado. Normalmente, el proceso de actualización es un proceso manual que suele llevar un tiempo para ser aplicado.

Técnicas de programación inseguras: Debido a los requerimientos de complejidad inherentes a un entorno de control, muchas implementaciones están desarrolladas con código inseguro. Por otro lado, muchas aplicaciones han sido desarrolladas por personal sin nociones sobre seguridad, lo que puede llevar a un sistema a sufrir ataques derivados de esta vulnerabilidad.

Dispositivos IT en redes industriales: Dispositivos como notebooks y servidores son un elemento común en las redes industriales. Estos elementos tienen sistemas operativos con vulnerabilidades conocidas, los cuales pueden causar daños colaterales en la red industrial.

Defectos en la red: Las redes actuales, en especial las de los sistemas de control, tienen funcionalidades que han sido desplegadas sin un análisis de seguridad suficiente y pueden ofrecer acceso a los atacantes una vez descubiertos.

Protocolo OPC: El protocolo OPC es un protocolo inseguro. Está basado en la tecnología DCOM de Microsoft, cuya seguridad se ha visto comprometida hasta el punto de que ya no se utiliza en entornos IT. Si bien es cierto que el protocolo OPC UA soluciona las carencias de seguridad del protocolo OPC, en el 90% de las instalaciones todavía se utiliza OPC.

Ataques a bases de datos: Los servidores de bases de datos se han convertido en las aplicaciones centrales de un sistema de control debido a la información que almacenan. Estos deben seguir las prácticas de seguridad adecuadas.

Capacidad de memoria y procesamiento limitada: Los dispositivos de campo están diseñados con una capacidad de procesamiento y memoria limitada al fin para el cual han sido diseñados. Este diseño tiene como ventajas un diseño robusto que soporta un ciclo de vida más largo y un costo de implementación y mantenimiento menor. Además, al tener opciones limitadas, la probabilidad de un error de seguridad por parte del operador también es limitada. Por otro lado, el costo de dicha simplicidad conlleva que estos dispositivos, en la gran mayoría de casos, no se puedan actualizar o parchear. Su software y hardware no soportan la instalación de mejoras de seguridad.

	Procedimientos de ciberseguridad: Con la integración de las redes y el aumento de la complejidad de las operaciones, el personal que tiene acceso a la red también ha aumentado. Se deben desarrollar y mantener alineados con el negocio unos procedimientos de ciberseguridad robustos.
	Tecnologías de seguridad IT en entornos industriales: Las tecnologías de seguridad IT en entornos industriales pueden ser un potencial punto de falla debido a la latencia que generan o por la posible interrupción del soporte por parte del proveedor al añadir dispositivos intermedios como firewalls o sistemas de detección de intrusiones (IDS).

Tabla 1 - Tipos de vulnerabilidades lógicas

Métodos para la detección de vulnerabilidades

En la actualidad, las organizaciones enfrentan una constante amenaza de ciberataques y vulnerabilidades que pueden afectar la integridad, confidencialidad y disponibilidad de sus activos críticos. Por ello, es esencial contar con métodos proactivos de evaluación que permitan identificar y corregir posibles vulnerabilidades en los sistemas de información y en la infraestructura de red.

Existen diversas técnicas para identificar y evaluar vulnerabilidades en sistemas de seguridad, como las pruebas de penetración, las evaluaciones de seguridad y el análisis crítico de código. Estas prácticas son útiles para identificar posibles amenazas y medir la resistencia de los sistemas frente a ataques, lo que permite tomar medidas preventivas y mitigar los riesgos. Sin embargo, es importante tener en cuenta que no todas las técnicas son adecuadas para todos los tipos de redes, ya que algunas pueden ser disruptivas y afectar la disponibilidad de los sistemas, un factor crítico en redes industriales que será abordado más adelante en este trabajo de tesis.

A continuación, se detallan algunos de los métodos proactivos de evaluación mencionados anteriormente para comprender el estado actual de la organización en cuanto a vulnerabilidades.

- **Herramientas automatizadas para la búsqueda e identificación de las vulnerabilidades:** Son programas diseñados para realizar pruebas de seguridad y detectar de forma automática vulnerabilidades en un sistema, generando informes detallados de los problemas identificados. Estas herramientas son capaces de analizar y correlacionar la información obtenida para comprobar de manera eficiente las vulnerabilidades encontradas. Han evolucionado a lo largo del tiempo y su base de conocimiento incluye la mayoría de las vulnerabilidades conocidas.
- **Evaluación y pruebas de seguridad**: La evaluación y las pruebas de seguridad son procesos fundamentales en la gestión de vulnerabilidades. La evaluación de la vulnerabilidad implica una primera revisión para identificar posibles vulnerabilidades en un sistema. Los resultados y la información obtenida durante esta evaluación se utilizarán para llevar a cabo las pruebas de seguridad. Estas pruebas buscan explotar las vulnerabilidades potenciales identificadas en la evaluación y verificar su grado de criticidad y explotabilidad. Ambos procesos son esenciales para garantizar la seguridad de los sistemas y prevenir posibles ataques o intrusiones.
- **Prueba de invasión:** Una de las metodologías proactivas para evaluar la seguridad de una organización es la prueba de invasión, también conocida como pentest. Esta prueba tiene como objetivo comprobar la resistencia de los activos de la organización frente a métodos de ataque conocidos. La prueba de invasión se lleva a cabo simulando un ataque real y utilizando técnicas de hacking ético para identificar y explotar vulnerabilidades en los sistemas de la organización. La prueba de invasión es una herramienta importante para identificar vulnerabilidades y mejorar la seguridad de la organización.
- **Análisis crítico de código:** El análisis crítico de código es una técnica que se utiliza para identificar vulnerabilidades y errores en el código fuente de un software o aplicación. Esta técnica implica un análisis detallado de cada línea de código para detectar posibles errores, debilidades y vulnerabilidades que puedan ser explotadas por atacantes malintencionados.

5. Identificación de las consecuencias

La identificación de las consecuencias potenciales de un incidente de seguridad es un componente fundamental en la gestión de vulnerabilidades, ya que permite a la organización comprender el impacto que un incidente puede tener en los activos críticos del negocio. La fase de evaluación del riesgo es la encargada de llevar a cabo esta tarea y consiste en comparar los niveles de riesgo identificados en la fase anterior (análisis del riesgo) con los criterios de evaluación y aceptación del riesgo definidos previamente.

Es importante que durante la evaluación del riesgo, la organización considere la importancia de los procesos de negocio o la actividad soportada por determinado activo o conjunto de activos. Si un proceso o actividad se valora como de baja importancia, los riesgos asociados a él deben ser también menos tenidos en cuenta que los riesgos que causan impactos en procesos o actividades más importantes.

Ciberseguridad en entornos Industriales

La constante evolución tecnológica ha permitido una mayor integración de dispositivos y sistemas en los procesos industriales, lo que ha aumentado significativamente la exposición a riesgos de seguridad. Por ende, la ciberseguridad industrial se ha convertido en un tema crítico en la protección de los activos y procesos de las organizaciones.

En el contexto de las organizaciones industriales, la seguridad, integridad y disponibilidad son aspectos fundamentales para garantizar el correcto funcionamiento de los procesos. Sin embargo, en la actualidad, los activos industriales se encuentran expuestos a un creciente número de ciberataques, lo que puede tener graves repercusiones en la conectividad de los sistemas OT, tales como los PLCs, SCADA, DCS, entre otros. Por esta razón, es imperativo llevar a cabo una evaluación exhaustiva de los sistemas relacionados con el proceso industrial con el fin de identificar las posibles vulnerabilidades de ciberseguridad y gestionarlas, a fin de contar con la información y capacidades suficientes para la aplicación de contramedidas que mitiguen los riesgos.

Ante las preocupaciones por la ciberseguridad en el ámbito industrial, los entes reguladores han identificado la necesidad de implementar medidas para mejorar la seguridad en las organizaciones, por ejemplo, el Parlamento Europeo adoptó en 2018 la Directiva de Seguridad de Redes y Sistemas de Información (NIS Directive), que se ha convertido en ley en la mayoría de los países de la UE, con el objetivo de abordar esta necesidad crítica.

Esto se complementa con las directrices de la Agencia Europea de Ciberseguridad (ENISA) y con la norma IEC 62443. Asimismo, en Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST), la Corporación de Regulación Eléctrica Nacional (NERC) y el Departamento de Seguridad Nacional (DHS) han publicado diversas directrices y normas.

Metodologías y técnicas a utilizar

La tesis de maestría llevará a cabo una investigación aplicada utilizando el método exploratorio descriptivo con el objetivo de probar la hipótesis planteada y cumplir con los objetivos generales y específicos propuestos. Para ello, se buscarán puntos de contraste que permitan detectar oportunidades de mejora y fundamentar el problema para obtener conclusiones válidas y confiables.

En cuanto a las técnicas específicas que se utilizarán para la recolección de información, se llevará a cabo una revisión sistemática de bibliografía proveniente de publicaciones científicas y académicas en revistas, congresos, conferencias y otros recursos relevantes en la temática. La recolección y síntesis de literatura permitirá producir evidencia suficiente para sustentar el marco teórico de la tesis de maestría.

En relación al proceso de investigación, se sustentará en conocimientos empíricos relevantes obtenidos a partir de la experiencia y el ejercicio profesional del autor en el ámbito de la seguridad informática industrial. En términos generales, se emplearán metodologías rigurosas y técnicas adecuadas para asegurar la validez y confiabilidad de los resultados obtenidos.

Estado del arte

La sección de "Estado del arte" tiene un rol importante en la investigación, ya que permite situar el problema en un contexto más amplio y comprender los avances y desarrollos que se han llevado a cabo en el área temática en la que se encuentra la investigación.

En esta sección, se abordará el panorama actual de la investigación en gestión de vulnerabilidades en entornos de OT, aunque es importante señalar que el estado del arte específico en este ámbito es limitado. Por tanto, se recurrirá a los avances y conocimientos existentes en la gestión de vulnerabilidades en entornos de IT como punto de referencia.

El análisis del estado del arte en gestión de vulnerabilidades en entornos IT proporcionará una base sólida de conceptos y enfoques metodológicos utilizados para identificar, evaluar y mitigar vulnerabilidades en sistemas. A partir de este análisis, se llevará a cabo una adaptación y construcción específica para los entornos OT, teniendo en cuenta las particularidades inherentes a estos sistemas y su interacción con los procesos industriales.

Este enfoque permitirá identificar las similitudes y diferencias entre la gestión de vulnerabilidades en entornos IT y OT, estableciendo así un marco conceptual robusto para la implementación efectiva de un proceso de gestión de vulnerabilidades en entornos OT.

Mediante la integración de los avances existentes en la gestión de vulnerabilidades en IT con las necesidades y desafíos propios de los entornos OT, se desarrollará un enfoque integral y adaptado que garantice la seguridad y la continuidad operativa de las instalaciones industriales.

Funciones principales de la gestión de vulnerabilidades

La gestión de vulnerabilidades desempeña un papel fundamental en la protección y fortalecimiento de los sistemas de seguridad. Esta gestión se basa en cuatro principales funciones, según lo señalado por (SYNNEX Westcon-Comstor, 2020), las cuales se detallan a continuación:

- **Descubrir**: Esta función se centra en la detección activa de errores, debilidades y fallos en los sistemas y aplicaciones. Implica llevar a cabo escaneos regulares de seguridad para identificar posibles vulnerabilidades. Una vez detectadas, se busca corregirlas o solucionarlas de manera oportuna para reducir los riesgos que podrían ser explotados por actores maliciosos. El objetivo es garantizar la integridad y la seguridad de los activos y los datos de la organización.
- **Informar**: La función de informar implica la generación de informes detallados sobre las vulnerabilidades descubiertas y las medidas necesarias para abordarlas. Estos informes sirven como guía para la toma de decisiones y permiten establecer acciones correctivas y preventivas. Además, proporcionan una visión clara del estado de seguridad de los sistemas y permiten evaluar la efectividad de las medidas de protección implementadas.
- **Priorizar**: Esta función se enfoca en determinar la prioridad de las vulnerabilidades descubiertas y las acciones a tomar en función de factores como la criticidad, el impacto potencial, la probabilidad de explotación y los recursos disponibles. Es importante establecer un orden de abordaje para garantizar que los recursos se asignen de manera eficiente y que los riesgos más críticos se mitiguen primero. Esto ayuda a optimizar la gestión de vulnerabilidades y a maximizar la protección de los activos de la organización.
- **Responder**: La función de responder se refiere a la implementación de medidas correctivas y preventivas para abordar las vulnerabilidades identificadas. Esto implica corregir los errores, debilidades o fallos descubiertos, mitigando el riesgo asociado. Además, se toman medidas para reducir las probabilidades de que las vulnerabilidades vuelvan a ocurrir en el futuro, lo que incluye fortalecer los controles de seguridad, actualizar los sistemas y aplicaciones, y capacitar al personal en buenas prácticas de seguridad.

En conjunto, estas funciones de gestión de vulnerabilidades permiten mantener un enfoque proactivo en la protección de los sistemas y datos de una organización, reduciendo los riesgos y mejorando la seguridad de manera continua. Al aplicar estas funciones de manera efectiva, se logra una mayor resiliencia y se minimiza la exposición a posibles amenazas y ataques cibernéticos.

Procesos de gestión de vulnerabilidades a través de escaneos

En la actualidad, muchas organizaciones no llevan a cabo escaneos de vulnerabilidades con la frecuencia necesaria, limitándose a realizarlos de forma trimestral o anual, lo que les otorga una visión momentánea del estado de seguridad de su entorno. Esta práctica, si bien permite identificar algunos riesgos potenciales, no es suficiente para garantizar una protección adecuada frente a amenazas cada vez más sofisticadas y cambiantes.

Es necesario destacar que las vulnerabilidades no son estáticas en el transcurso del tiempo, sino que presentan un carácter dinámico y evolutivo. Este fenómeno se atribuye a diversos factores, como el envejecimiento de los activos, la obsolescencia tecnológica y la aparición continua de nuevas amenazas en el ámbito de la seguridad informática. Como consecuencia de estos elementos, las vulnerabilidades tienden a aumentar en cantidad y gravedad si no se les concede la atención y el tratamiento adecuados de manera periódica.

A medida que transcurre el tiempo, los sistemas y aplicaciones se vuelven más susceptibles a los avances y sofisticación de las técnicas de ataque empleadas por actores malintencionados. Por ende, resulta imperativo adoptar un enfoque de gestión de vulnerabilidades constante y proactivo, que incluya la realización de evaluaciones periódicas, la implementación de actualizaciones de seguridad y un seguimiento continuo de los sistemas. Solo mediante este enfoque riguroso es posible salvaguardar eficazmente los activos, preservar la integridad de los procesos y mitigar los riesgos asociados a las vulnerabilidades en el entorno de seguridad informática.

La figura siguiente muestra un posible ciclo de vida de las vulnerabilidades con un escaneo con frecuencia anual:

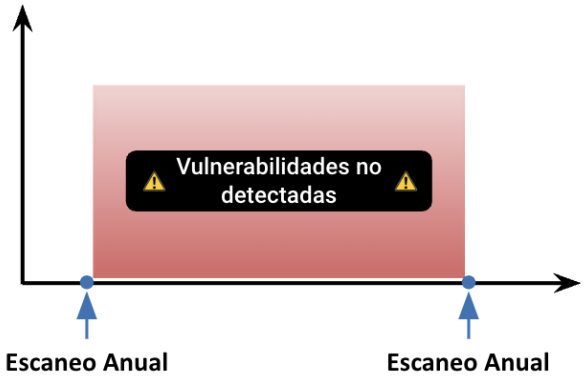

Figura 3 - Escaneo con frecuencia anual

En el actual esquema, existe la posibilidad de que una vulnerabilidad no sea detectada durante el escaneo programado, lo que implica que los sistemas podrían permanecer expuestos a riesgos durante períodos prolongados. Con el fin de mitigar este riesgo, resulta fundamental implementar un proceso de gestión de vulnerabilidades que incluya una frecuencia de escaneo más frecuente, a fin de reducir el tiempo de exposición de los sistemas y asegurar una detección oportuna de posibles vulnerabilidades emergentes. La siguiente figura presenta un esquema detallado de este enfoque, destacando la importancia de una estrategia proactiva para la gestión de vulnerabilidades.

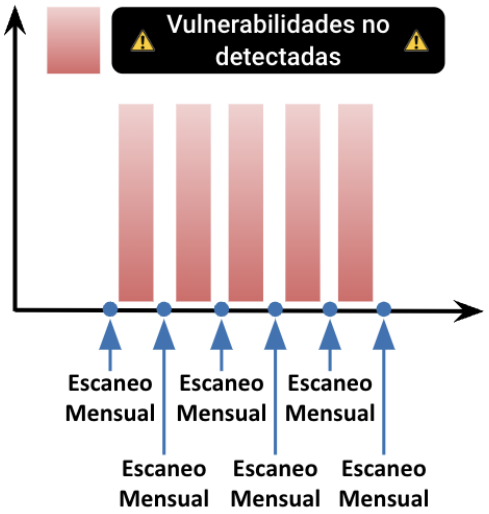

Figura 4 - Escaneo con frecuencia mensual

La implementación de este proceso de gestión de vulnerabilidades permite mitigar de manera significativa los riesgos a los que una organización se enfrenta, al posibilitar la identificación y remediación proactiva de cualquier vulnerabilidad en los sistemas antes de que sea explotada por amenazas externas. Mediante la implementación de un plan de revisión mensual, el cual se ajusta de manera continua hasta alcanzar la ventana de mantenimiento programada, se garantiza la detección temprana y la aplicación oportuna de medidas correctivas.

Para garantizar una efectiva gestión de vulnerabilidades, es fundamental que la estrategia implementada esté alineada con el nivel de madurez en ciberseguridad de la organización. En el caso de una entidad que aún no ha implementado medidas de seguridad, resulta poco factible llevar a cabo un escaneo completo de vulnerabilidades de manera mensual. Sin embargo, se pueden realizar ajustes iterativos durante la ventana de mantenimiento mensual, con el propósito de abordar progresivamente las vulnerabilidades detectadas.

Roles y responsabilidades

La definición precisa de los roles y responsabilidades en el proceso de gestión de vulnerabilidades reviste una importancia fundamental para garantizar la efectividad y coherencia en la ejecución de las tareas asignadas. En base al tamaño y nivel de complejidad de la organización, es posible que las personas desempeñen múltiples roles simultáneamente, adaptándose a las necesidades y características propias del proceso.

Es esencial establecer una estructura claramente definida que identifique los roles y responsabilidades de cada individuo involucrado en la gestión de vulnerabilidades. Esto permitirá que cada persona comprenda claramente sus funciones y obligaciones, así como las expectativas en términos de desempeño. Al asignar los roles de manera adecuada, se facilitará una coordinación eficiente de los esfuerzos y se minimizará el riesgo de duplicación de tareas o falta de responsabilidad en la ejecución del proceso.

A continuación, se detallan los roles clave que deben estar definidos dentro del proceso de gestión de vulnerabilidades:

Responsable de seguridad
El Responsable de Seguridad desempeña un rol fundamental como el propietario del proceso de gestión de vulnerabilidades. Su responsabilidad es el diseño y la implementación efectiva de dicho proceso, asegurando que se cumplan los objetivos establecidos. Como líder del equipo de seguridad, tiene la tarea de establecer las políticas y directrices que guiarán la gestión de vulnerabilidades en la organización. Esto implica la definición de los procedimientos, la asignación de recursos y la supervisión de las actividades relacionadas con la identificación, evaluación y mitigación de las vulnerabilidades existentes.
Ingeniero de vulnerabilidades
El rol de ingeniero de vulnerabilidades se encarga de configurar y administrar las herramientas de revisión de vulnerabilidades (escáner de vulnerabilidades), así como de programar y ejecutar las tareas necesarias para detectar posibles debilidades en los sistemas y aplicaciones.
Propietario del activo
El propietario del activo es responsable es el responsable de supervisar y evaluar el activo que será analizado por la herramienta de gestión de vulnerabilidades. Su función principal es analizar los resultados del análisis de riesgo y proponer medidas de mitigación, tomando en cuenta el impacto y buscando un acuerdo con el responsable de seguridad para su implementación.
Ingeniero de mitigación y remediación
La función de este rol es aplicar las medidas necesarias para mitigar y/o remediar las vulnerabilidades detectadas.

Tabla 2 - Roles del proceso de gestión de vulnerabilidades en entornos IT

Proceso de gestión de vulnerabilidades

El proceso de gestión de vulnerabilidades se compone de cinco etapas esenciales, en las cuales los roles previamente definidos tienen un papel fundamental. Cada etapa está diseñada para abordar de manera organizada la detección, evaluación y mitigación efectiva de las vulnerabilidades presentes en los sistemas de la organización. A continuación, se detallan las actividades y responsabilidades asociadas a cada etapa, proporcionando una visión estructurada del proceso de gestión de vulnerabilidades (Palmaers, 2021):

1) Definición y planificación del alcance.
2) Configuración de la herramienta de revisión de vulnerabilidades y ejecución del proceso de revisión.
3) Definición de contramedidas para mitigar o corregir las vulnerabilidades.
4) Implementación de contramedidas para mitigar o corregir las vulnerabilidades.
5) Escaneo de vulnerabilidades de verificación.

En la gestión de vulnerabilidades, dentro de la fase de definición del alcance se establece la frecuencia de ejecución de las actividades en cada una de las etapas del proceso. Durante esta fase, se determina la periodicidad con la que se llevarán a cabo las actividades de detección, evaluación y mitigación de vulnerabilidades.

Es importante destacar que la periodicidad establecida en la fase de definición del alcance no es estática y puede ser modificada a lo largo del tiempo. A medida que evolucionan las amenazas y los sistemas, es necesario revisar y ajustar la frecuencia de las actividades para garantizar una gestión efectiva de las vulnerabilidades.

1) Definición y planificación del alcance.

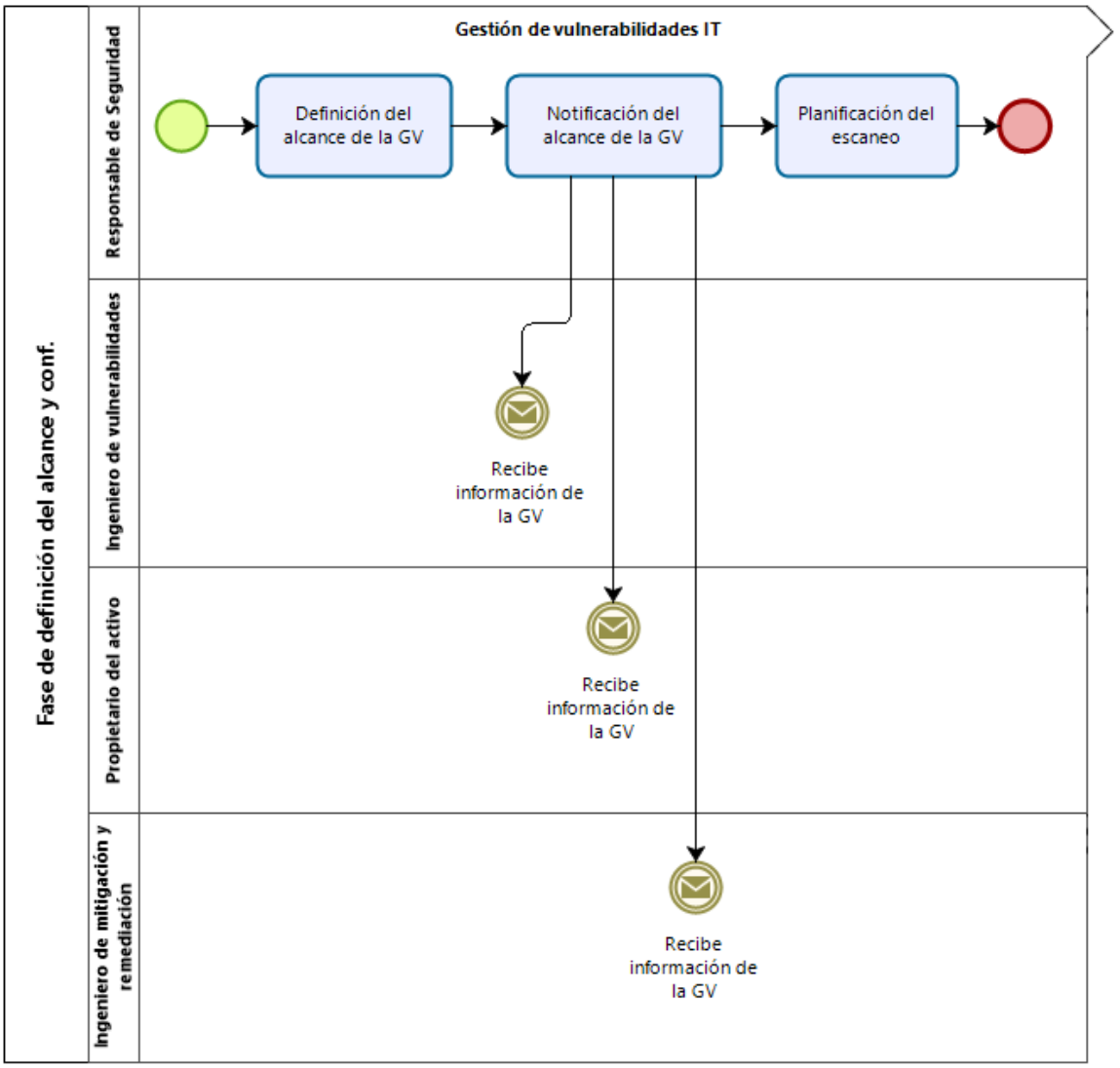

Figura 5 - Definición y planificación del alcance[8]

En esta fase es importante definir con precisión el alcance de la herramienta de revisión de vulnerabilidades para maximizar su efectividad del trabajo. El responsable de seguridad tiene como función elaborar una lista exhaustiva de sistemas y activos que van a ser alcanzados por la herramienta.

[8] En el diagrama se incluyen las siglas "GV", las cuales representan la abreviatura de Gestión de Vulnerabilidades.

Se debe tener en cuenta que los escaneos con autenticación pueden tener limitaciones y riesgos, por lo que se debe evaluar cuidadosamente su necesidad y seguir las mejores prácticas. Combinar escaneos internos y externos permite obtener una visión más completa del estado de seguridad de la organización.

Después de determinar el alcance, el responsable de seguridad debe informar a los propietarios de los activos, quienes son responsables de identificar acciones correctivas para mitigar las vulnerabilidades. Se deben detallar los objetivos del proceso de gestión de vulnerabilidades, así como las responsabilidades de los propietarios de activos en todo el proceso.

Es importante informar también a la oficina responsable de administrar equipos de infraestructura y planificar los escaneos de vulnerabilidad. Dependiendo de la configuración del escáner, se pueden realizar diferentes tipos de escaneos que relevan mayor o menor información, lo que puede impactar el equipo escaneado. Por último, se debe notificar a los equipos de supervisión de seguridad para evitar falsos positivos en las alertas generadas por las herramientas de escaneo de vulnerabilidades.

2) **Configuración de la herramienta de revisión de vulnerabilidades y ejecución del proceso de revisión.**

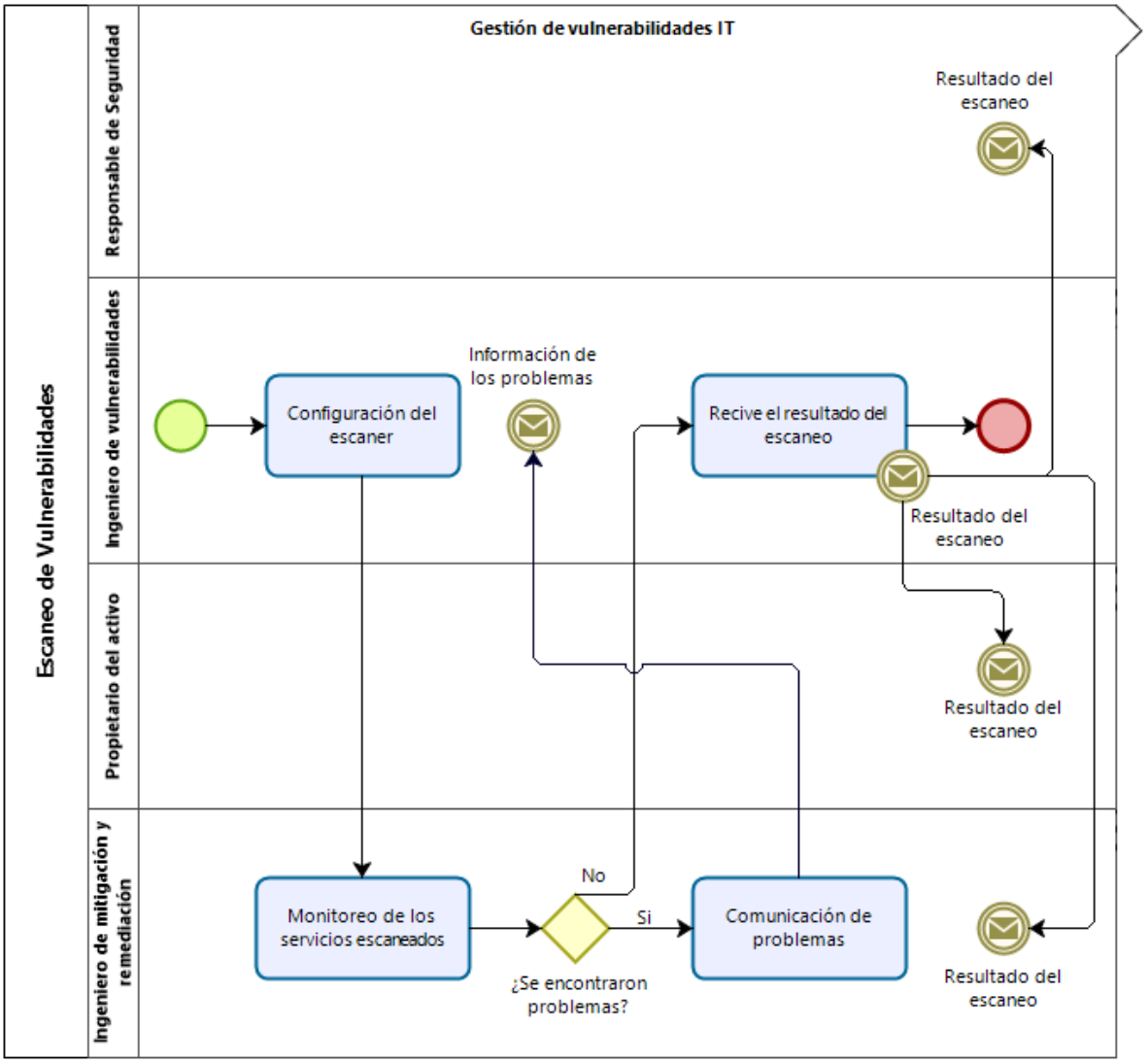

Figura 6 - Configuración de la herramienta de revisión de vulnerabilidades y ejecución del proceso de revisión

La fase de escaneo de vulnerabilidades tiene como objetivo detectar la existencia de debilidades en los sistemas y aplicaciones. El Ingeniero de Vulnerabilidades debe configurar el escáner con los parámetros previamente definidos para reducir la generación de falsos positivos.

Durante esta fase, el Ingeniero de mitigación y remediación debe supervisar los servicios escaneados para garantizar que no se interrumpan. Cualquier problema que surja debe registrarse para tomar medidas y reducir el impacto en futuros escaneos.

Luego, en la fase de evaluación de vulnerabilidades, se analizan los resultados del escaneo para identificar las vulnerabilidades presentes en los sistemas y aplicaciones. El responsable de seguridad debe presentar una evaluación de riesgos con recomendaciones para mitigar las vulnerabilidades identificadas a los propietarios de los activos.

Finalmente, los propietarios de los activos son responsables de autorizar las acciones correctivas necesarias y definir plazos para su implementación. Es importante realizar un seguimiento periódico para garantizar que se implementen de manera efectiva y se mantenga la seguridad de los sistemas y aplicaciones. En conclusión, la fase de escaneo de vulnerabilidades es crítica para garantizar la seguridad de los sistemas y aplicaciones y debe llevarse a cabo con cuidado y diligencia.

3) Definición de contramedidas para mitigar o corregir las vulnerabilidades

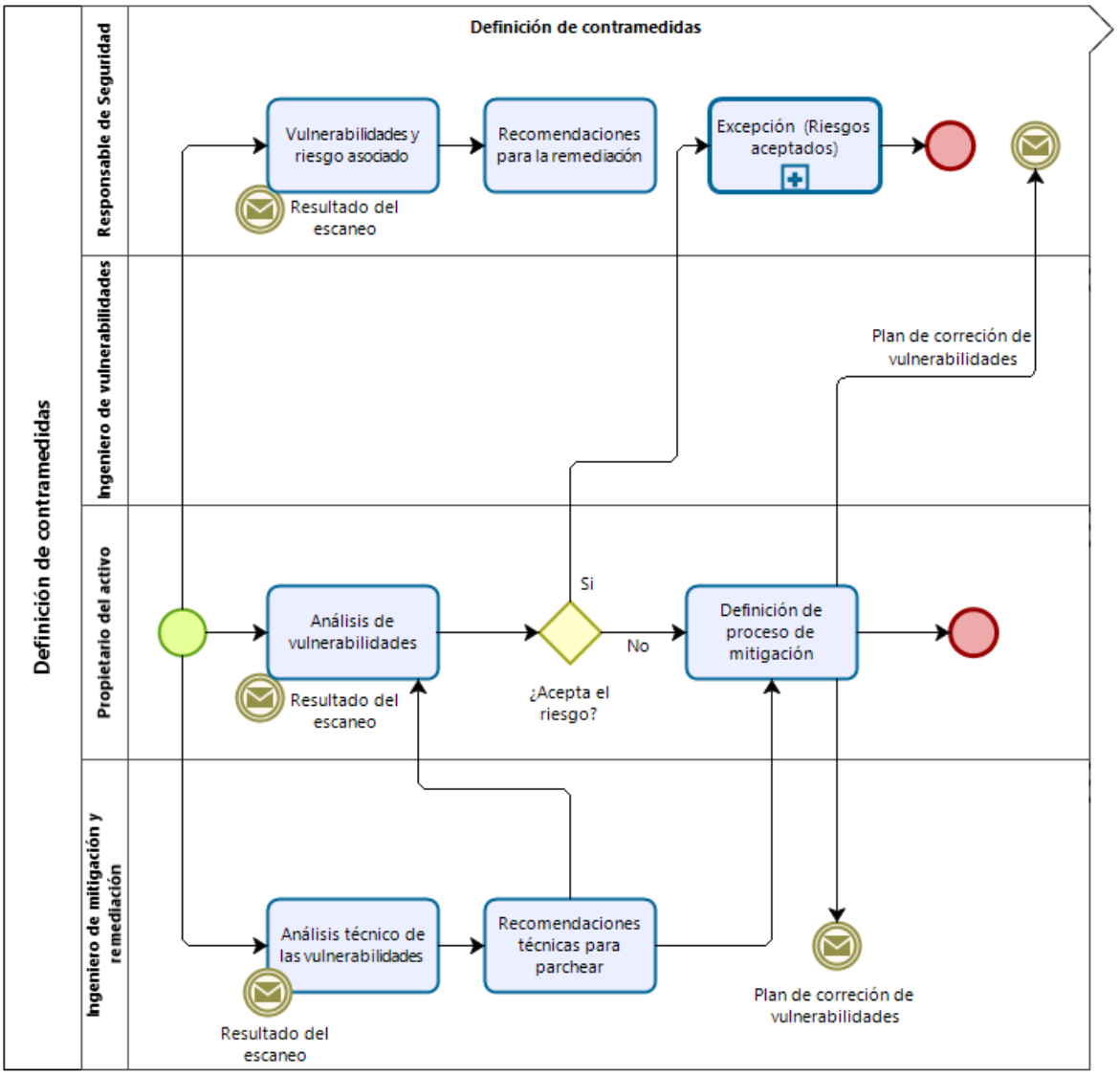

Figura 7 - Definición de contramedidas para mitigar o corregir las vulnerabilidades

En la fase de definición de contramedidas, los propietarios de los activos en conjunto con el Responsable de Seguridad y el Ingeniero de mitigación y remediación son los responsables de tomar decisiones para mitigar o corregir las vulnerabilidades identificadas. Durante esta etapa, se evalúan varias soluciones y se seleccionan las medidas más adecuadas en función de la criticidad de las vulnerabilidades, los recursos disponibles y los plazos establecidos.

Con el fin de evitar impactos no deseados, es necesario llevar a cabo una evaluación exhaustiva de las contramedidas seleccionadas y analizar detalladamente las posibles consecuencias que podrían derivar de su implementación.

Es importante establecer un plan de seguimiento para evaluar la efectividad de las contramedidas implementadas y hacer ajustes en caso de ser necesario. La colaboración y coordinación entre los propietarios de activos, el responsable de seguridad y el equipo de ingeniería es fundamental para garantizar una gestión adecuada y eficaz de las vulnerabilidades.

El responsable de seguridad es responsable de analizar las vulnerabilidades desde un punto de vista de negocio, determinando los riesgos asociados y aportando sus recomendaciones sobre la corrección de las vulnerabilidades. Posterior a la definición del plan de acción, el rol que deberá cumplir es el de encargado, realizando seguimiento de las medidas definidas.

El Ingeniero de mitigación y remediación es responsable de analizar las vulnerabilidades desde un punto de vista técnico y definir los plazos para la aplicación de parches o contramedidas que corrijan las vulnerabilidades.

El propietario del activo es responsable de definir las fechas para la ejecución del plan de acción para la aplicación de parches o contramedidas[9] que corrijan las vulnerabilidades. El plazo definido debe estar alineado con el nivel de riesgo detectado en cada uno de los activos.

[9] En este trabajo, se utilizan indistintamente los términos "contramedidas", "medidas de seguridad" y "controles compensatorios" para hacer referencia a las acciones implementadas con el objetivo de mitigar o prevenir riesgos y vulnerabilidades en un sistema o entorno determinado. Estos términos son utilizados de manera intercambiable para describir las diversas medidas y enfoques adoptados para proteger los activos, sistemas y datos de una organización frente a posibles amenazas y ataques cibernéticos.

En algunos casos, no es posible realizar una remediación de las vulnerabilidades en el corto plazo, por lo que se deben definir controles compensatorios[10] para mitigar o eliminar el riesgo sin corregir la vulnerabilidad.

Los riesgos considerados elevados, dependiendo de la organización, solo pueden ser aceptados por la alta dirección, mientras que los riesgos de menor magnitud pueden ser aceptados por los propietarios de los activos, siempre y cuando estén por debajo del umbral establecido para la aceptación del riesgo. Es fundamental documentar adecuadamente estas decisiones y sus fundamentos para mantener una gestión efectiva de los riesgos.

[10] Los controles compensatorios son contramedidas alternativas diseñadas para reducir las vulnerabilidades en situaciones en las que la contramedida originalmente propuesta no puede ser aplicada debido a limitaciones o restricciones. Estos controles, en conjunto, buscan compensar la falta de implementación de la contramedida original y brindar un nivel adecuado de protección.

4) Implementación de contramedidas para mitigar o corregir las vulnerabilidades

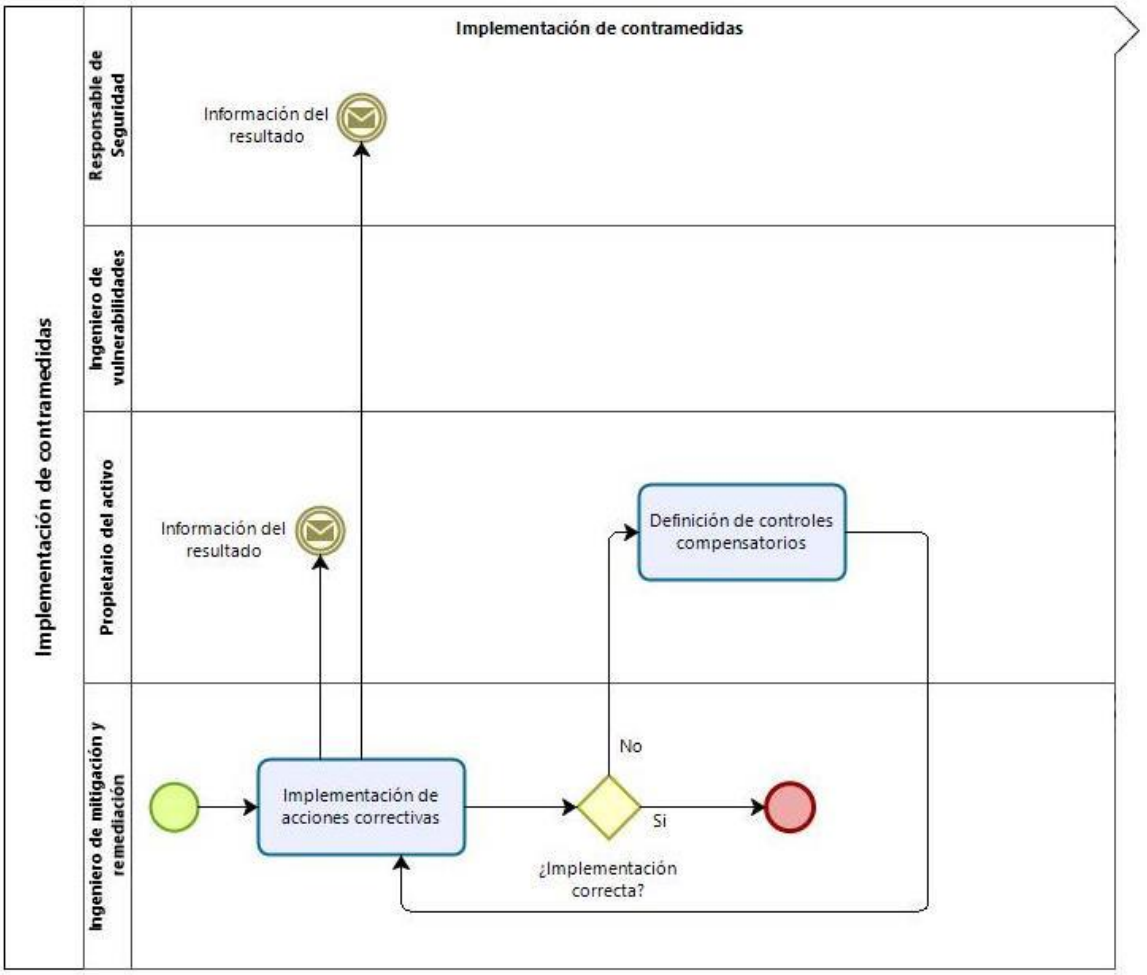

Figura 8 - Implementación de contramedidas para mitigar o corregir las vulnerabilidades

Para asegurar una gestión eficiente de la seguridad de los activos, se debe llevar a cabo la implementación de las contramedidas para mitigar o corregir las vulnerabilidades en los plazos establecidos en el plan de acción acordado. De esta manera, se garantiza una respuesta rápida y eficaz ante posibles amenazas y se minimiza el impacto en la organización.

No obstante, en caso de que se presenten problemas con las medidas implementadas, es esencial que se documenten detalladamente y que el propietario del activo tome la decisión de definir las medidas alternativas también llamadas controles compensatorios basadas en las recomendaciones del responsable de seguridad y del ingeniero de mitigación y remediación.

Estas medidas alternativas deben ser cuidadosamente evaluadas y aplicadas para garantizar que se aborden las vulnerabilidades de manera efectiva y se protejan los activos de la organización.

Además, el responsable de seguridad debe asegurarse de realizar un seguimiento periódico del estado de las medidas implementadas, con el fin de garantizar que siguen siendo efectivas en el tiempo y que se mantienen actualizadas frente a nuevas amenazas y vulnerabilidades que puedan surgir. Este seguimiento debe ser realizado de manera constante y rigurosa para asegurar la integridad y disponibilidad de los activos y la continuidad del negocio.

5) Escaneo de vulnerabilidades de verificación

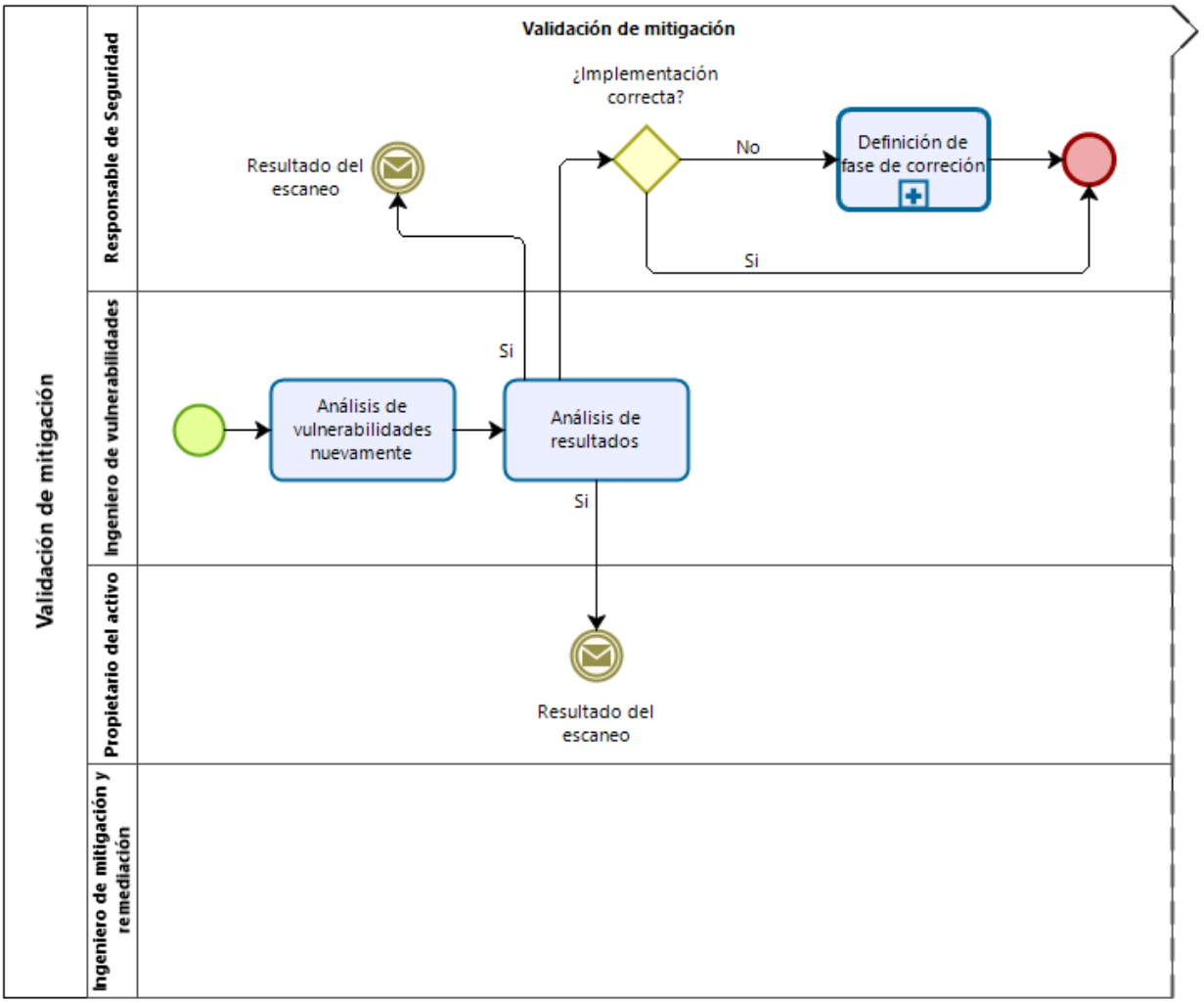

Figura 9 - Escaneo de vulnerabilidades de verificación

Al finalizar la implementación del plan de acción para mitigar o corregir las vulnerabilidades, resulta importante realizar una verificación mediante un escaneo de vulnerabilidades para confirmar que se han aplicado correctamente las acciones definidas en el plan.

Este escaneo debe realizarse utilizando las mismas herramientas de escaneo de vulnerabilidades y los mismos ajustes de configuración utilizados en el escaneo inicial, a fin de evitar resultados imprecisos debido a errores de configuración.

Los escaneos de validación se planifican después de la fecha límite establecida para implementar los parches o contramedidas correspondientes a las vulnerabilidades detectadas en la fase de "Implementación de contramedidas para mitigar o corregir las vulnerabilidades".

En el contexto de estos escaneos, es importante mantener el mismo formato en la generación de los informes que se utilizó durante el escaneo inicial. El propósito de esto es realizar un seguimiento riguroso y validar la efectividad de las acciones implementadas, así como identificar cualquier riesgo residual que pueda existir.

En resumen, la verificación a través de un nuevo escaneo de vulnerabilidades es una etapa necesaria del proceso de gestión de vulnerabilidades, ya que permite asegurar que las contramedidas medidas correctivas aplicadas han sido efectivas en la eliminación de las vulnerabilidades y, por tanto, minimizar los riesgos de seguridad.

Solución propuesta

En esta tesis de maestría, se presenta una metodología para la gestión de vulnerabilidades en entornos industriales que busca disminuir el impacto en la continuidad del proceso industrial al aplicar contramedidas de software/firmware. La propuesta incluye un rol existente en la organización, el **rol del área de operaciones**, el cual será responsable de los equipos de campo, se involucre en el proceso de gestión de vulnerabilidades como parte de la ciberseguridad.

Este rol del área de operaciones desempeñará la función de coordinar con la oficina de seguridad las ventanas de mantenimiento de los equipos de campo, evitando interrupciones en el proceso industrial. Este enfoque mejora significativamente la postura general de la organización en términos de ciberseguridad, al involucrar a las áreas industriales que desempeñan un papel crucial en la continuidad operativa y el éxito del negocio, y que hasta el momento no contaban con un proceso formal de gestión de vulnerabilidades.

Es importante destacar que, dependiendo de la organización, se pueden requerir aprobaciones formales de los propietarios de los activos antes de realizar escaneos de vulnerabilidades.

Estos propietarios pueden tener requisitos específicos que abarcan desde la realización de escaneos únicamente durante las ventanas de mantenimiento de los sistemas de producción hasta la preferencia de realizarlos exclusivamente durante las horas de trabajo, cuando el personal técnico está presente. Esto se debe a que, en caso de surgir algún inconveniente o impacto generado por la herramienta de escaneo, se cuenta con recursos disponibles para solucionarlo de manera inmediata. Estos requisitos reflejan la importancia de considerar el contexto operativo y las capacidades de respuesta de la organización al planificar y ejecutar los escaneos de vulnerabilidades.

La definición de ventanas mencionada anteriormente es uno de los aspectos clave que distingue a las redes de propósito general, como las redes IT, de los entornos industriales. En las redes IT, los escaneos de vulnerabilidades suelen llevarse a cabo fuera del horario laboral, en períodos más amplios, aprovechando momentos de menor actividad para minimizar el impacto en la operación regular.

Por tanto, es esencial establecer una política clara para las ventanas de mantenimiento y tomar medidas para evitar cualquier potencial impacto negativo en el proceso industrial. Con esta metodología, se espera **mejorar significativamente la gestión de vulnerabilidades en entornos industriales** y disminuir al máximo posible el riesgo de interrumpir la continuidad de los procesos críticos para la organización.

La inclusión del rol del área de operaciones en el proceso de gestión de vulnerabilidades representa un avance significativo para lograr una mayor coordinación y eficacia en la ciberseguridad de los entornos industriales. Al contar con la participación activa del área de operaciones, se promueve una comprensión de los sistemas y procesos industriales, lo que facilita la identificación y abordaje efectivo de las vulnerabilidades.

Esta estrecha colaboración entre los equipos de ciberseguridad y el área de operaciones permite una respuesta más rápida y precisa ante posibles incidentes de ciberseguridad, garantizando la protección de los activos críticos de la organización. En conjunto, esta integración fortalece la postura de ciberseguridad y contribuye a la continuidad operativa de los entornos industriales.

En base a lo expuesto previamente, la solución propuesta para abordar la problemática de gestión de vulnerabilidades en entornos industriales implica la realización de actividades clave que requieren una atención detallada. Estas actividades incluyen la **definición de roles y responsabilidades** claras y bien definidas, la **descripción de alto nivel del proceso de gestión de vulnerabilidades** y el establecimiento de un **flujo de trabajo efectivo para la gestión y validación de contramedidas**. A su vez, se llevará a cabo el **desarrollo integral del proceso de gestión de vulnerabilidades** adaptado a las particularidades de los entornos industriales.

Actividades previas al detalle de proceso de gestión de vulnerabilidades

Roles y responsabilidades

El establecimiento de roles y responsabilidades es un elemento fundamental en la gestión de vulnerabilidades. Tal como se menciona en el capítulo "Estado del Arte", se deben definir y asignar las tareas correspondientes a cada actor involucrado en el proceso de gestión de vulnerabilidades.

Es importante tener en cuenta que, en diversos entornos organizativos, tanto de pequeñas como grandes empresas, es común que los profesionales designados desempeñen múltiples roles de manera simultánea. Esto implica que pueden estar involucrados en diferentes tareas y responsabilidades dentro del contexto de la gestión de vulnerabilidades. Por tanto, resulta se deben adaptar los roles y las responsabilidades según las necesidades y características específicas de cada organización, teniendo en cuenta factores como la estructura organizativa, los procesos internos y el entorno tecnológico.

Esta flexibilidad en la asignación de roles contribuye a optimizar el aprovechamiento de los recursos humanos, favoreciendo así la eficiencia en la gestión y la alineación efectiva con los objetivos y desafíos propios de cada organización.

Una organización que busca llevar a cabo una gestión de vulnerabilidades efectiva en entornos operativos debería contar con los siguientes roles y responsabilidades claramente definidos:

Responsable de seguridad

El Responsable de Seguridad desempeña un rol importante ya que es el propietario del proceso de gestión de vulnerabilidades. Su responsabilidad es el diseño y la implementación efectiva de dicho proceso, asegurando que se cumplan los objetivos establecidos. Como líder del equipo de seguridad, tiene la tarea de establecer las políticas y directrices que guiarán la gestión de vulnerabilidades en la organización, para lo cuál debe contar con conocimiento del proceso industrial y los equipos de campo que intervienen. El rol tiene como alcance la definición de los procedimientos, la asignación de recursos y la supervisión de las actividades relacionadas con la identificación, evaluación y mitigación de las vulnerabilidades existentes.

Ingeniero de vulnerabilidades

El rol de ingeniero de vulnerabilidades se encarga de configurar y administrar las herramientas de revisión de vulnerabilidades (escáner de vulnerabilidades), así como de programar y ejecutar las tareas necesarias para detectar posibles debilidades en los sistemas y aplicaciones. Para la gestión de vulnerabilidades de entornos industriales debe contar con conocimiento de los equipos de campo los protocolos y puertos que utilizan, como así también las particularidades de cada uno.

Responsable del proceso industrial

Es la persona encargada de la supervisión y gestión del proceso industrial en la organización. Este rol tiene la responsabilidad de garantizar el correcto funcionamiento y la continuidad operativa del proceso, así como de tomar decisiones relacionadas con la implementación de medidas de seguridad y la gestión de vulnerabilidades. El responsable del proceso industrial trabaja en estrecha colaboración con otros roles, como el responsable de seguridad, para asegurar que las operaciones se realicen de manera segura y eficiente.

Propietario del activo OT

El propietario del activo es responsable es el responsable de supervisar y evaluar el activo que será analizado por la herramienta de gestión de vulnerabilidades. Su función principal es analizar los resultados del análisis de riesgo y proponer medidas de mitigación, tomando en cuenta el impacto y buscando un acuerdo con el responsable de seguridad para su implementación.

Ingeniero de mitigación y remediación
El ingeniero de mitigación y remediación debe contar con un sólido conocimiento técnico en sistemas industriales, protocolos de comunicación, dispositivos de campo y tecnologías relacionadas. Además, debe estar al tanto de las mejores prácticas de seguridad y de las últimas amenazas y vulnerabilidades relevantes para el entorno industrial. Trabaja en estrecha colaboración con otros roles, como el responsable de seguridad y el ingeniero de vulnerabilidades, para asegurar la implementación efectiva de las contramedidas y garantizar la continuidad operativa del proceso industrial.

Tabla 3 - Roles del proceso de gestión de vulnerabilidades en entornos OT

Proceso de gestión de vulnerabilidades industriales

Para llevar a cabo el proceso de gestión de vulnerabilidades en sistemas industriales, es necesario seguir un flujo detallado de cada actividad para evitar interrupciones en el proceso industrial.

Por tanto, se debe acordar una ventana de mantenimiento en la cual todas las partes involucradas estén de acuerdo en realizar el proceso de gestión de vulnerabilidades. Durante esta ventana de mantenimiento, se procederá a realizar el escaneo de vulnerabilidades en los activos de OT.

El escaneo de vulnerabilidades puede arrojar dos posibles resultados. El primer resultado es la ausencia de detección de vulnerabilidades. En este caso, el proceso de gestión de vulnerabilidades concluirá hasta la próxima ventana de mantenimiento acordada.

Cuando no se detectan vulnerabilidades, se considera un indicio positivo de que las medidas de seguridad implementadas hasta el momento están siendo efectivas. Sin embargo, es importante tener en cuenta que las amenazas y vulnerabilidades pueden evolucionar con el tiempo, por lo que es necesario realizar escaneos periódicos para garantizar la continuidad de la protección.

La próxima ventana de mantenimiento acordada se refiere al período programado en el cual se llevarán a cabo las actividades de mantenimiento y actualización de los sistemas y equipos.

Es importante destacar que la ausencia de vulnerabilidades en un escaneo no significa que el entorno esté completamente libre de riesgos. Se recomienda mantener una vigilancia constante y seguir las buenas prácticas de seguridad para asegurar la protección continua de los activos y la integridad del entorno operativo.

El segundo resultado es que se detecten vulnerabilidades. En este caso, es necesario registrarlas en el track de vulnerabilidades y comenzar con el proceso de gestión de vulnerabilidades. El proceso de gestión de vulnerabilidades incluirá la evaluación del riesgo de las vulnerabilidades detectadas, la priorización de las medidas de mitigación y/o remediación necesarias y la aplicación de dichas medidas. Una vez aplicadas las medidas necesarias, se realizará un escaneo de verificación de vulnerabilidades para verificar si se han eliminado todas las vulnerabilidades mitigadas.

La implementación de un control compensatorio para mitigar una vulnerabilidad registrada en el track de vulnerabilidades dependerá de la evaluación del riesgo asociado a dicha vulnerabilidad. Esta evaluación permitirá determinar si la vulnerabilidad es crítica y requiere una aplicación inmediata del control compensatorio, o si puede ser mitigada en una ventana de tiempo más amplia, ya sea a largo o mediano plazo.

La evaluación del riesgo involucra un análisis exhaustivo de diversos factores, como el impacto potencial de la vulnerabilidad en los activos y sistemas de la organización, la probabilidad de explotación por parte de un agente malicioso y la disponibilidad de recursos y capacidades para implementar el control compensatorio.

En caso de que la vulnerabilidad se considere crítica y presente un riesgo inmediato, se priorizará la implementación del control compensatorio de forma urgente. Esto permitirá reducir la exposición a posibles ataques y salvaguardar la integridad y disponibilidad de los activos y sistemas afectados.

Por otro lado, si la vulnerabilidad se evalúa como de menor impacto o presenta un riesgo mitigable a largo o mediano plazo, se programará su mitigación dentro de una ventana de tiempo adecuada. Esto implica asignar recursos y planificar las acciones necesarias para aplicar el control compensatorio de manera eficiente y efectiva.

Una vez finalizada la etapa de mitigación, se debe realizar una validación para garantizar que la vulnerabilidad haya sido mitigada de manera efectiva. Esta validación tiene como objetivo confirmar que los controles compensatorios mitigaron la vulnerabilidad detectada.

En caso de que la validación sea exitosa y se verifique que la vulnerabilidad ha sido mitigada de manera satisfactoria, se procede a actualizar el track de vulnerabilidades y se considera que el proceso ha sido concluido con éxito.

Sin embargo, en situaciones donde la aplicación del parche o el control compensatorio no ha sido aprobada durante la validación, se debe proceder a realizar un rollback. El rollback consiste en revertir los cambios realizados durante el proceso de mitigación con el fin de evitar posibles impactos en el proceso industrial y garantizar su correcto funcionamiento.

El rollback se lleva a cabo de manera cuidadosa y siguiendo los procedimientos establecidos para minimizar cualquier interrupción o deterioro en la operación del sistema. Es fundamental contar con planes de contingencia y protocolos de rollback bien definidos y validados previamente para abordar estas situaciones con el fin de poder restaurar el sistema a un estado anterior seguro y funcional.

Es importante destacar que tanto la validación como el rollback forman parte integral del proceso de gestión de vulnerabilidades y son fundamentales para asegurar la integridad y continuidad operativa de los sistemas en entornos industriales.

Flujo de trabajo para la gestión y validación de contramedidas

El diagrama de flujo que se presenta a continuación proporciona una guía visual para el flujo de trabajo en la gestión y validación de la aplicación de controles compensatorios, asegurando que las vulnerabilidades sean mitigadas de manera efectiva y garantizando la seguridad del sistema.

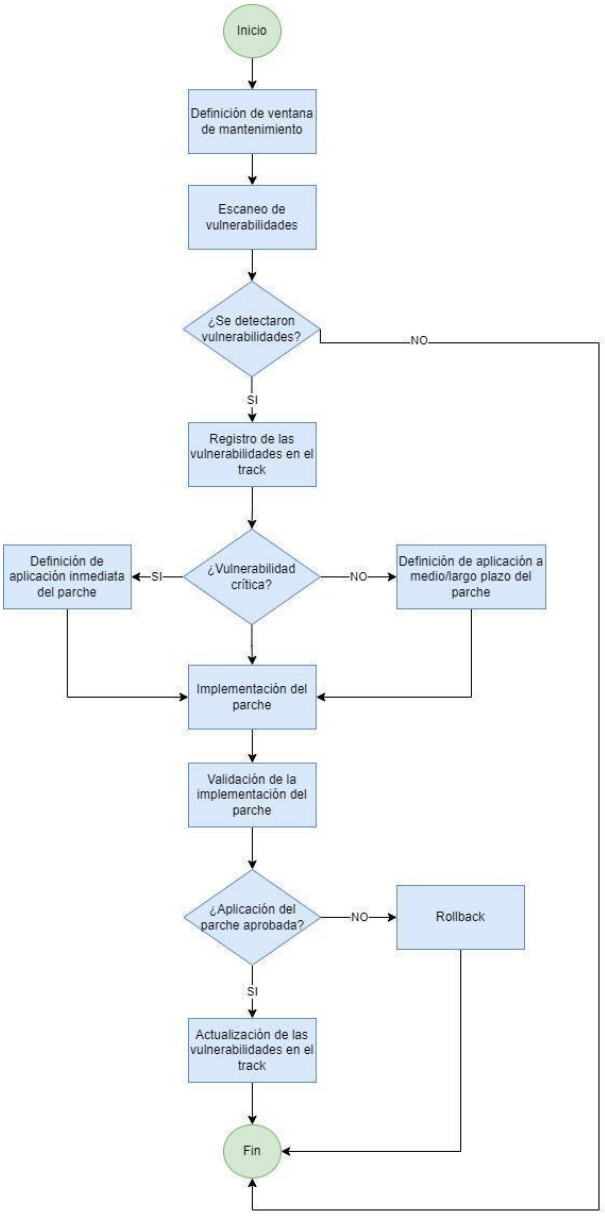

Figura 10 - Proceso de gestión de vulnerabilidades industriales

Desarrollo del proceso de gestión de vulnerabilidades en entornos industriales

En este proceso se examina en detalle el proceso de gestión de vulnerabilidades en entornos industriales. El enfoque se centra en las diferentes etapas que componen este proceso y cómo cada una de ellas contribuye de manera significativa a fortalecer la seguridad y salvaguardar los sistemas y aplicaciones críticos.

El proceso comienza abordando la etapa de definición y planificación del alcance, en la cual se establecen los objetivos y metas del proceso, así como los activos y sistemas que serán objeto de una revisión. A continuación, se profundiza en la configuración de la herramienta de revisión de vulnerabilidades y la ejecución del proceso de revisión.

Posteriormente, se explora la etapa de definición de contramedidas, en la cual se identifican y evalúan las vulnerabilidades detectadas, con el objetivo de establecer controles compensatorios o contramedidas..

Continuando con el análisis, se examina detenidamente la etapa de revisión y validación del plan de mitigación, donde se llevan a cabo revisiones exhaustivas y rigurosas pruebas para asegurar la eficacia y solidez de las contramedidas propuestas.

Además, se explora la importancia de una implementación precisa y adecuada de las contramedidas, haciendo énfasis en la necesidad de una supervisión constante y un seguimiento para garantizar la efectividad y continuidad de las medidas adoptadas.

Por último, se aborda la etapa de escaneo de vulnerabilidades de verificación, en la cual se realizan auditorías adicionales para confirmar la eficacia de las contramedidas implementadas y garantizar la protección sostenida de los sistemas a lo largo del tiempo.

Por lo tanto, la gestión de vulnerabilidades se divide en seis etapas, en las cuales participan los actores previamente definidos en la sección de "Roles y responsabilidades", tomando como base el flujo de trabajo para la gestión y validación de controles compensatorios establecido en la figura anterior (Figura 11).

A continuación, se detallan las actividades y responsabilidades asociadas a cada etapa:

1) Definición y planificación del alcance.
2) Configuración de la herramienta de revisión de vulnerabilidades y ejecución del proceso de revisión.
3) Definición de contramedidas para mitigar o corregir las vulnerabilidades.
4) Revisión y validación del plan de mitigación
5) Implementación de contramedidas para mitigar o corregir las vulnerabilidades.
6) Escaneo de vulnerabilidades de verificación.

1) Definición y planificación del alcance

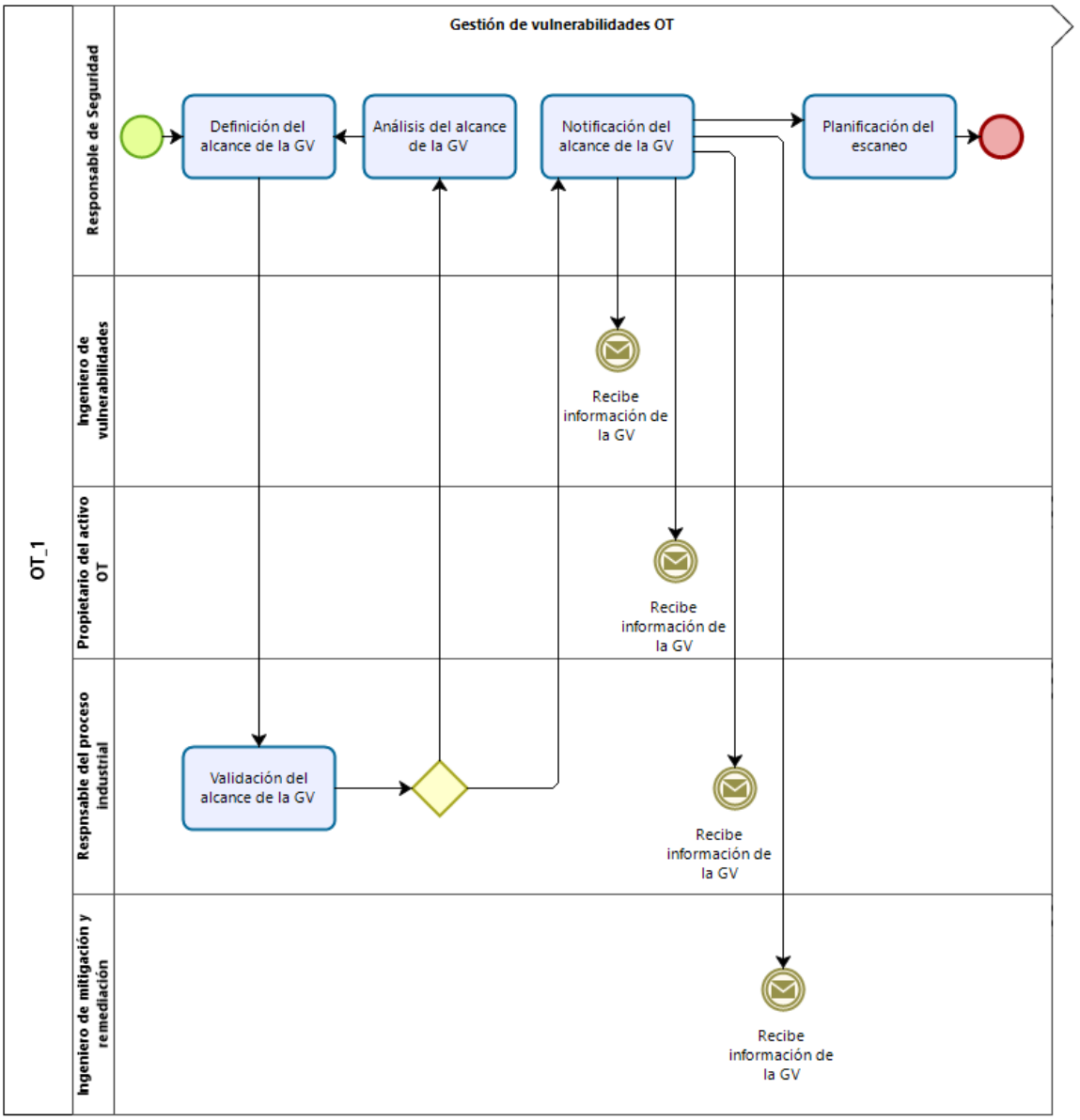

Figura 11 - Definición y planificación del alcance[11]

El proceso de gestión de vulnerabilidades en entornos industriales se compone de diversas etapas, siendo la primera la definición y planificación del alcance. En esta etapa inicial, se requiere un trabajo en conjunto entre el responsable de seguridad y el responsable del proceso industrial para establecer el alcance del escaneo de vulnerabilidades.

[11] En el diagrama se incluyen las siglas "GV", las cuales representan la abreviatura de Gestión de Vulnerabilidades.

La definición del alcance implica determinar qué sistemas, redes y activos de campo serán objeto de evaluación y análisis en busca de posibles vulnerabilidades. Esta tarea se realiza en función de la importancia y criticidad de los activos involucrados, así como de los riesgos asociados a su exposición. Una precisa definición del alcance, asegura que los escaneos se enfoquen en los activos más relevantes y críticos, optimizando así los recursos y esfuerzos dedicados a la gestión de vulnerabilidades.

Además, es necesario planificar los escaneos de vulnerabilidades en colaboración con el responsable del proceso industrial y el propietario del activo. Durante esta planificación, se definen aspectos como la frecuencia de los escaneos, el nivel de profundidad del análisis y la ventana de mantenimiento programada.

La frecuencia de los escaneos puede variar según la criticidad de los sistemas y las actualizaciones o cambios en el entorno industrial. Asimismo, el nivel de profundidad del análisis se determina en función de las necesidades de seguridad y los recursos disponibles. Por último, la ventana de mantenimiento programada se establece para minimizar cualquier impacto en las operaciones del proceso industrial durante los escaneos.

Es importante documentar adecuadamente la planificación de los escaneos de vulnerabilidades. Esta documentación permitirá tener una trazabilidad completa de las actividades realizadas en el proceso de gestión de vulnerabilidades, lo cual facilita la revisión, auditoría y seguimiento de las acciones llevadas a cabo. Además, la documentación proporciona transparencia y claridad en cuanto a los roles y responsabilidades de cada participante, los criterios utilizados en la definición del alcance y la planificación de los escaneos.

2) **Configuración de la herramienta de revisión de vulnerabilidades y ejecución del proceso de revisión**

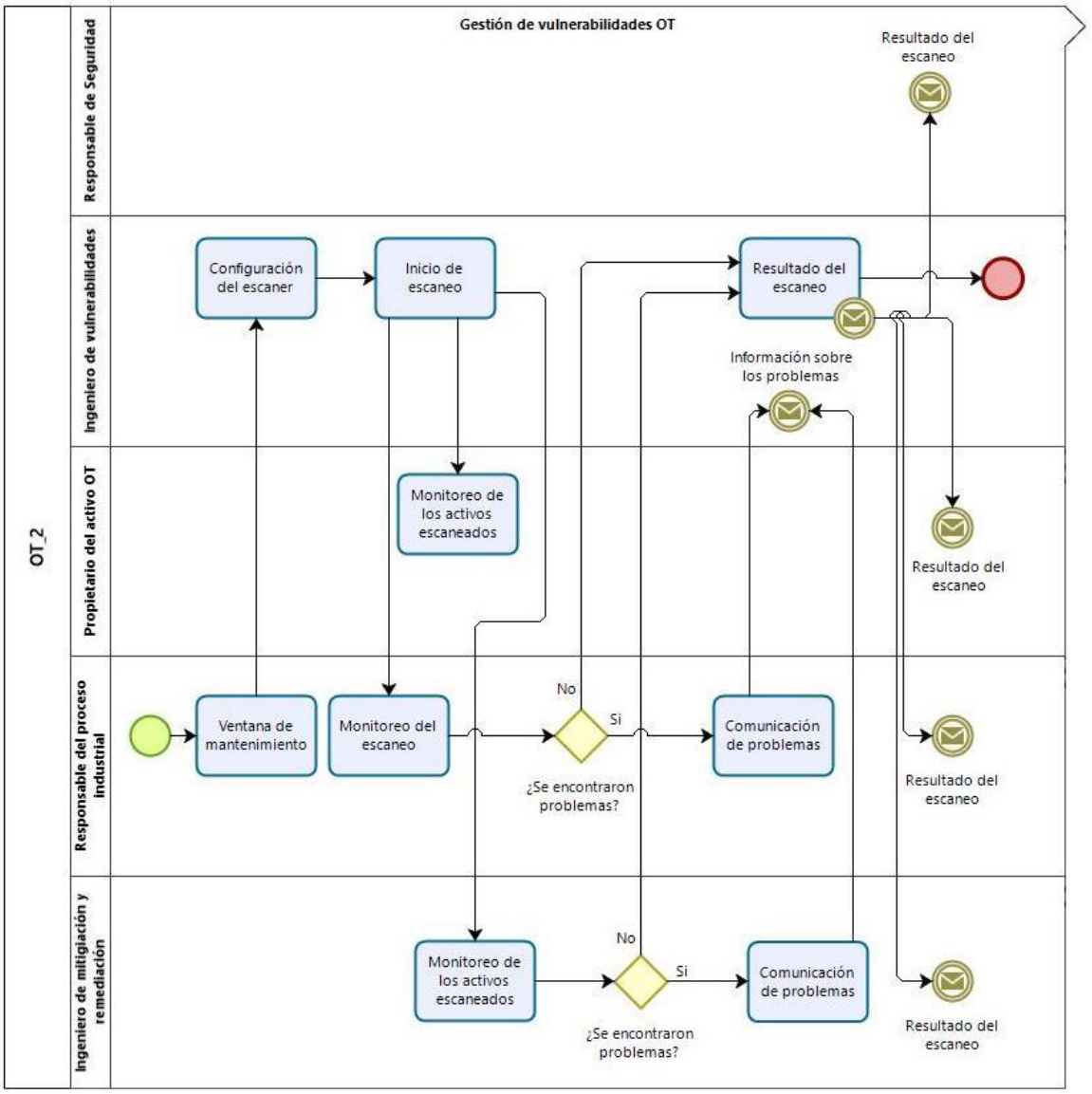

Figura 12 -Configuración de la herramienta de revisión de vulnerabilidades y ejecución del proceso de revisión.

La fase de configuración de la herramienta de revisión de vulnerabilidades es la segunda instancia en el proceso de identificación de vulnerabilidades en entornos industriales. Para lograr una obtención efectiva de vulnerabilidades, es un requerimiento que el responsable de la herramienta tenga un conocimiento detallado del entorno que será analizado y del funcionamiento del proceso. Esto le permitirá configurar adecuadamente todos los parámetros del equipo, garantizando así una configuración óptima para la detección y análisis de vulnerabilidades.

Los campos que deben considerarse para la configuración de la herramienta de revisión de vulnerabilidades incluyen lo siguiente:

Protocolo	En entornos industriales, a diferencia de los entornos de tecnología de la información, es común encontrar protocolos específicos y, en algunos casos, protocolos propietarios. Por tanto, es importante tener en cuenta esta diversidad de protocolos al configurar la herramienta de revisión de vulnerabilidades, asegurándose de que sea compatible con los protocolos utilizados en el entorno industrial objetivo. Esto permitirá realizar un escaneo efectivo y preciso de las vulnerabilidades presentes en los sistemas y dispositivos industriales.
Puerto	Los equipos de campo suelen utilizar puertos específicos dependiendo del proveedor y las necesidades del proceso industrial. Sin embargo, es importante tener en cuenta que los responsables de los equipos pueden realizar cambios en la configuración de los puertos. Por tanto, al configurar la herramienta de revisión de vulnerabilidades, se debe validar qué puertos están habilitados en cada equipo objetivo. Esto garantiza que la herramienta escanee los puertos relevantes y pueda identificar posibles vulnerabilidades asociadas a los servicios o aplicaciones que utilizan dichos puertos.

Slot de CPU (PLC)	Se debe realizar un relevamiento previo para validar si el PLC tiene algún módulo instalado en alguno de los slots disponibles. Esta información permite configurar correctamente la herramienta de revisión de vulnerabilidades, ya que se incluye dentro del alcance el escaneo de los slots ocupados por los módulos del PLC, lo cuál permite identificar y evaluar posibles vulnerabilidades que puedan afectar tanto al PLC como a los dispositivos conectados a PLC, brindando una visión integral de la seguridad del sistema.
Time out	El time out se refiere al tiempo máximo permitido para que el escáner espere una respuesta del dispositivo o sistema que está siendo escaneado. Se establece un límite de tiempo para cada solicitud de escaneo, y si no se recibe una respuesta dentro de ese período, se considera un time out. Configurar adecuadamente el time out es esencial para garantizar que el la herramienta de revisión de vulnerabilidades pueda completar el escaneo en un tiempo razonable y evitar bloqueos prolongados o retrasos en el proceso.
Nivel de intrusión	El nivel de intrusión se refiere al grado de intensidad o profundidad del escaneo realizado por la herramienta de vulnerabilidades. Este parámetro determina el alcance con la herramienta de revisión de vulnerabilidades interactúa con los dispositivos y sistemas. Un nivel de intrusión alto implica un escaneo más exhaustivo y profundo, mientras que un nivel de intrusión bajo implica un escaneo menos intrusivo y más superficial. La elección del nivel de intrusión depende de las necesidades y políticas de seguridad de la organización, así como de las características y vulnerabilidades conocidas de los sistemas que se están escaneando.

Autenticación	La autenticación se refiere al proceso de proporcionar las credenciales adecuadas para acceder a los dispositivos y sistemas que serán escaneados. La autenticación puede ser necesaria para obtener un acceso más profundo y exhaustivo a los activos de la red y descubrir vulnerabilidades que de otra manera no serían visibles. Existen diferentes métodos de autenticación que pueden ser configurados en la herramienta de revisión de vulnerabilidades, como: ● Credenciales locales: Se utilizan las credenciales de usuario y contraseña específicas del dispositivo o sistema que se va a escanear. Estas credenciales son proporcionadas a la herramienta de revisión de vulnerabilidades para que pueda autenticarse y realizar el escaneo. ● Credenciales de dominio: Se utilizan las credenciales de usuario y contraseña de un dominio de red para acceder a los dispositivos y sistemas. Esto es común en entornos empresariales donde se utiliza un dominio de Active Directory para administrar los accesos. ● Certificados de autenticación: En algunos casos, se pueden utilizar certificados digitales para autenticar la herramienta de revisión de vulnerabilidades ante los dispositivos y sistemas. Estos certificados son emitidos por una autoridad de certificación confiable y permiten establecer una comunicación segura y autenticada.

Tabla 4 - Campos para la configuración de la herramienta de detección de vulnerabilidades

Durante la ventana de mantenimiento programada, el ingeniero encargado de las vulnerabilidades en entornos industriales inicia el proceso de revisión de las vulnerabilidades. El responsable del proceso industrial en conjunto con el responsable del activo de OT y el ingeniero de mitigación y remediación supervisan los equipos que están alcanzados por el proceso. El objetivo principal es asegurar que los servicios no se vean interrumpidos y que las operaciones continúen sin contratiempos.

Durante el proceso de escaneo, es importante registrar cualquier incidente o problema que se presente. Esto incluye la falta de disponibilidad de los equipos de campo, respuestas deficientes o cualquier otro comportamiento inesperado. Estos registros proporcionan una valiosa información para la toma de decisiones y permiten tomar medidas preventivas y correctivas en futuros escaneos.

3) **Definición de contramedidas para mitigar o corregir las vulnerabilidades**

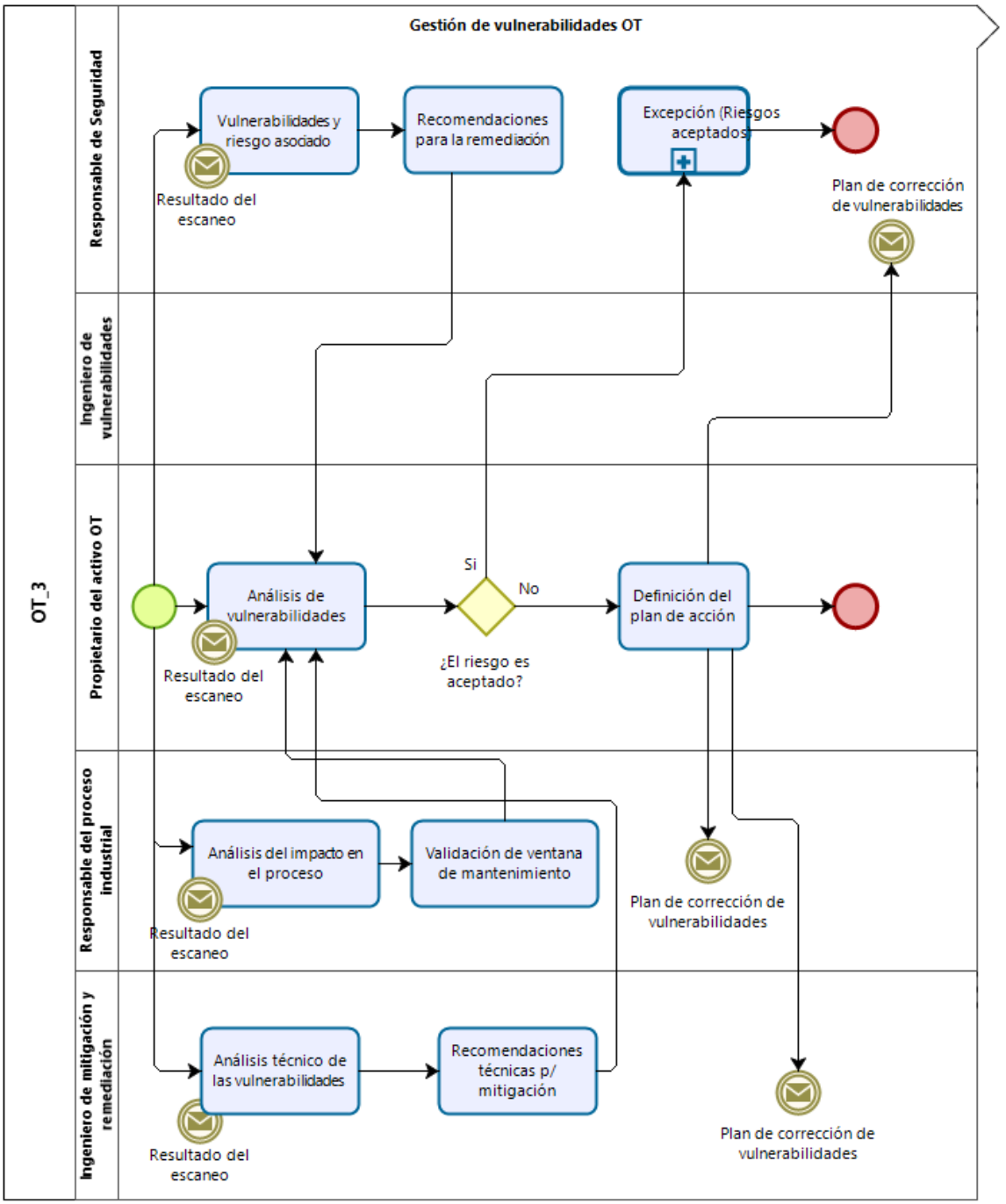

Figura 14 - Definición de contramedidas para mitigar o corregir las vulnerabilidades

En la fase de definición de contramedidas para mitigar o corregir las vulnerabilidades en entornos industriales, es responsabilidad de los propietarios de los activos OT, en colaboración con otros roles, tomar decisiones estratégicas y operativas.

El Responsable de Seguridad tiene como función principal analizar las vulnerabilidades desde una perspectiva de negocio, evaluando los riesgos asociados y el posible impacto en caso de que se explote la vulnerabilidad. Además, se encarga de proporcionar un detalle preciso del proceso y hacer recomendaciones sobre las medidas correctivas necesarias.

Por otro lado, el Responsable del Proceso Industrial tiene la responsabilidad de colaborar estrechamente con el propietario del activo OT para determinar la ventana de mantenimiento más adecuada en función del tipo de implementación que se va a realizar. Su objetivo es garantizar la continuidad de las operaciones mientras se llevan a cabo las acciones de mitigación.

El Propietario del Activo OT debe definir las fechas para la ejecución del plan de acción destinado a aplicar los parches o contramedidas necesarias para corregir las vulnerabilidades identificadas. Estas fechas deben estar alineadas con el nivel de riesgo detectado en cada uno de los activos, asegurando así una respuesta adecuada y oportuna.

Por último, el Ingeniero de Mitigación y Remediación desempeña un papel técnico. Su responsabilidad principal radica en analizar las vulnerabilidades desde una perspectiva técnica, proporcionando detalles sobre el proceso de aplicación de parches o actualización de firmware en los equipos. Además, es importante que este ingeniero defina un plan de rollback o contingencia en caso de que ocurran fallas o se presente algún comportamiento inesperado durante el proceso de mitigación. Asimismo, se encarga de establecer los plazos para la aplicación de parches o contramedidas que solucionen las vulnerabilidades.

En determinadas circunstancias, puede resultar inviable abordar directamente la remediación de vulnerabilidades debido a restricciones físicas de los equipos involucrados. En estos casos, es imperativo **implementar controles compensatorios** que posibiliten la mitigación o eliminación del riesgo asociado sin necesidad de abordar directamente la vulnerabilidad en sí.

Los controles compensatorios mencionados previamente también se aplican en casos donde no se puede definir una ventana de mantenimiento a corto plazo o cuando no se dispone de los recursos financieros necesarios para llevar a cabo la mitigación. En el contexto de los PLC, la actualización del firmware puede requerir asimismo la actualización del software de programación asociado, lo cual implica también el costo de obtener una licencia de software.

Es importante destacar que la implementación de controles compensatorios debe ser considerada como una medida temporal y que, en la medida de lo posible, se deberá buscar oportunidades para abordar la vulnerabilidad de forma definitiva en el futuro. Estos controles pueden incluir, por ejemplo, la implementación de medidas de seguridad adicionales en la red, la segmentación de la infraestructura, el monitoreo y detección de actividad maliciosa, entre otros enfoques.

La selección y diseño de los controles compensatorios debe realizarse de manera cuidadosa, considerando el nivel de riesgo y los impactos potenciales en el entorno industrial. Asimismo, se debe documentar adecuadamente la justificación y el seguimiento de los controles compensatorios implementados, a fin de mantener un registro completo de las acciones tomadas para mitigar los riesgos asociados a las vulnerabilidades no remediadas.

Sin perder de foco en la **gestión de riesgos en entornos industriales**, la evaluación y aceptación de riesgos en un entorno organizacional involucra un proceso que requiere la participación y toma de decisiones de diferentes niveles de la organización. En este sentido, los riesgos que se consideran de alta magnitud, según la perspectiva de la compañía, únicamente pueden ser aceptados por la alta dirección. Esto implica que la máxima instancia de gobierno de la empresa debe tomar conocimiento y asumir la responsabilidad de estos riesgos más significativos.

Por otro lado, los riesgos de menor envergadura pueden ser asumidos por los propietarios de los activos, siempre y cuando se encuentren por debajo del umbral previamente establecido para la aceptación del riesgo. Esta asignación de responsabilidad es posible debido a que los propietarios de los activos están más cercanos a las operaciones y tienen un conocimiento detallado de los riesgos asociados a sus activos específicos. No obstante, es importante destacar que incluso estos riesgos de menor magnitud deben ser evaluados y documentados de manera adecuada para garantizar una gestión efectiva y transparente de los riesgos en la organización.

La documentación de las decisiones de aceptación de riesgos y los fundamentos que las respaldan es un elemento clave dentro del proceso de gestión de riesgos. Esta práctica permite tener un registro claro y completo de las decisiones tomadas, los criterios utilizados y las justificaciones pertinentes. Además, proporciona una base sólida para la comunicación, el monitoreo y la revisión continua de los riesgos aceptados. La documentación adecuada no solo respalda la trazabilidad, sino que también facilita la identificación de áreas de mejora y la retroalimentación para futuras evaluaciones de riesgo.

4) Revisión y validación del plan de mitigación

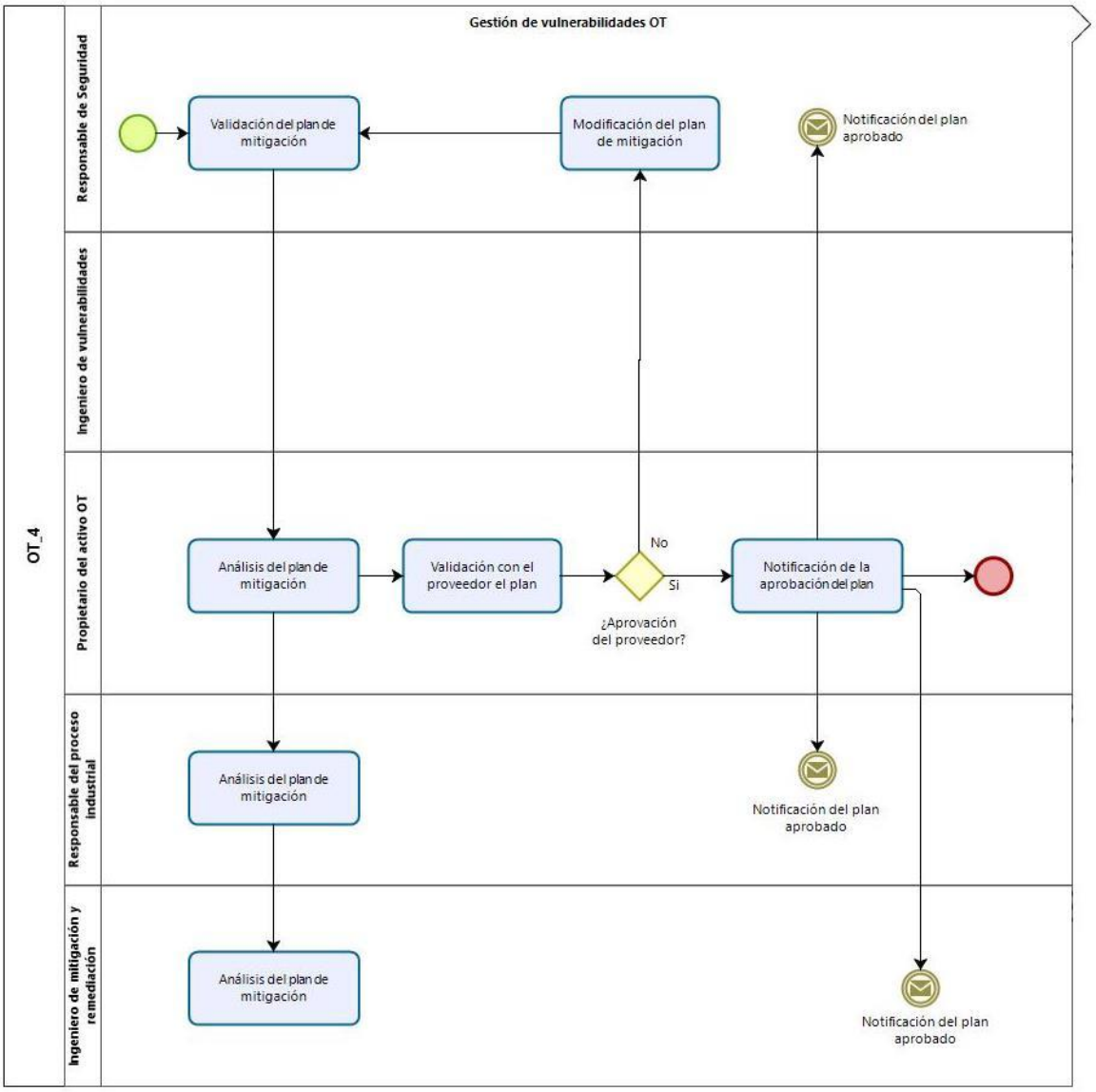

Figura 14 - Revisión y validación del plan de mitigación

La etapa de revisión y validación del plan de mitigación tiene un rol fundamental para asegurar la efectividad y viabilidad de las acciones propuestas. Este paso intermedio implica la revisión detallada del plan de mitigación por parte de las partes interesadas, tanto internas como externas.

La remediación de vulnerabilidades en un entorno OT puede requerir la colaboración de proveedores externos, ya que su experiencia y conocimiento especializado pueden ser necesarios para implementar las soluciones adecuadas.

Por tanto, en esta fase de revisión, se busca obtener la retroalimentación y el aporte de los proveedores para garantizar que las acciones propuestas sean factibles y cumplan con los estándares de seguridad requeridos.

Sin embargo, la validación del plan de mitigación no se limita solo a la participación de los proveedores externos. También es esencial obtener el acuerdo interno de todas las partes involucradas, incluido el responsable de riesgos o aquellos con un conocimiento profundo del impacto de aplicar o no aplicar las correcciones propuestas. En este sentido, se evalúan cuidadosamente las implicaciones de cada medida de mitigación y se consideran factores como la criticidad de los activos, los costos asociados, la continuidad operativa y otros aspectos relevantes.

Es importante tener en cuenta que, en algunos casos, no todas las correcciones propuestas se aplicarán de manera total. La validación del plan de mitigación permite una evaluación exhaustiva de cada acción y su impacto potencial. Esto significa que se realizará un análisis riguroso para determinar qué correcciones son prioritarias y cuáles pueden postergarse o requerir un enfoque diferente.

5) **Implementación de contramedidas para mitigar o corregir las vulnerabilidades**

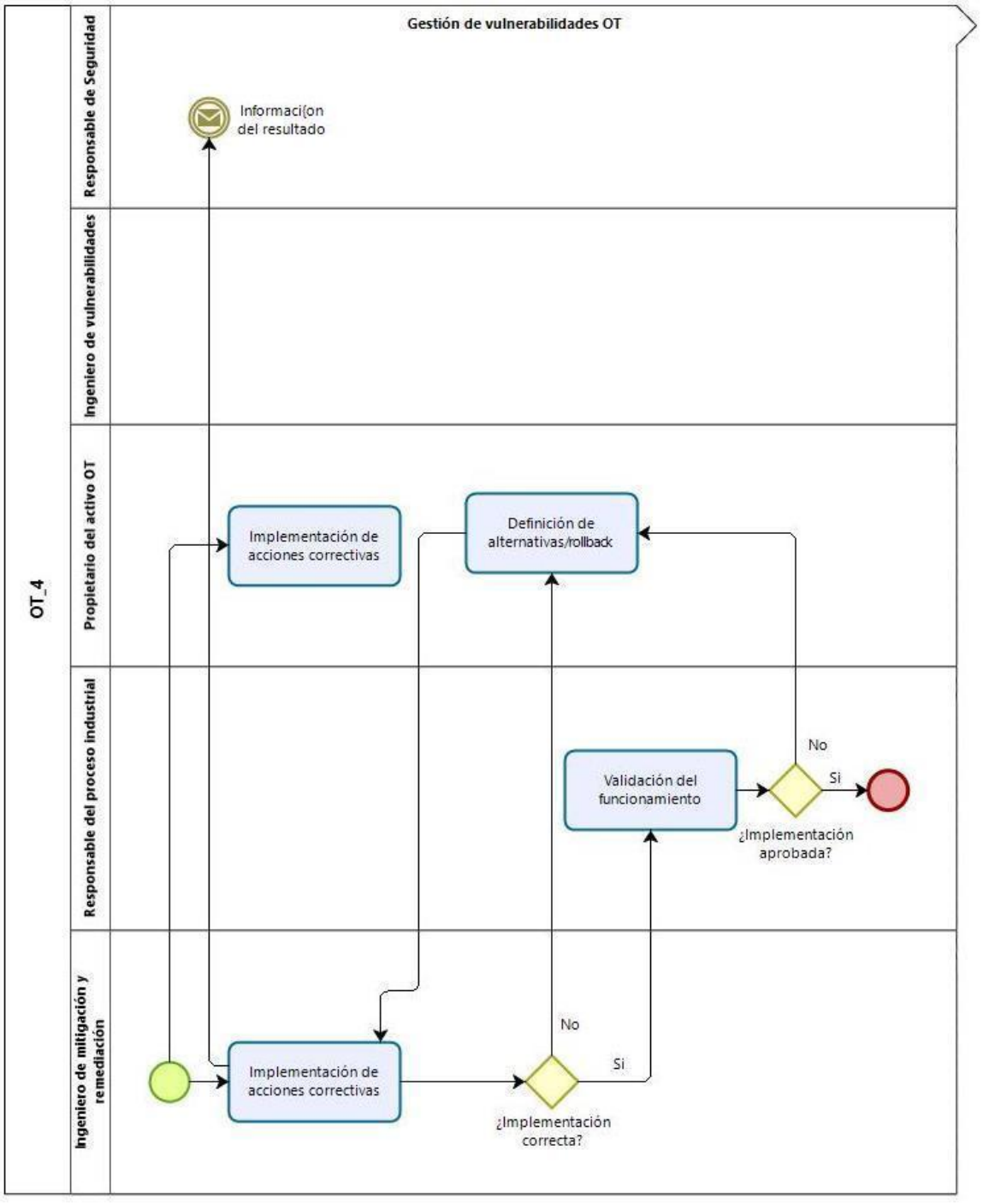

Figura 15 - Implementación de contramedidas para mitigar o corregir las vulnerabilidades

Para llevar a cabo el plan de acción detallado para cada una de las vulnerabilidades identificadas en la fase anterior, se debe coordinar la implementación de las contramedidas en ventanas de mantenimiento programadas, en caso de ser necesarias. Esta etapa implica realizar cambios y modificaciones en el entorno industrial con el objetivo de mitigar el riesgo asociado a las vulnerabilidades identificadas.

Durante la implementación de contramedidas, es importante estar preparados para enfrentar posibles desafíos y garantizar la continuidad del proceso industrial. Para ello, se debe establecer un plan de contingencia que incluya la posibilidad de realizar un rollback en caso de que surjan problemas que afecten el funcionamiento del sistema. Este enfoque proactivo permite revertir rápidamente los cambios implementados y asegurar que el proceso industrial vuelva a su estado operativo anterior.

Una vez finalizado el proceso de aplicación de las contramedidas, el Responsable de Seguridad tiene la responsabilidad de realizar un seguimiento constante del estado de las medidas implementadas. Esto implica evaluar regularmente la efectividad de las contramedidas y su capacidad para proteger el sistema industrial contra futuros ataques. Además, se deben realizar evaluaciones periódicas para asegurar que las contramedidas sigan siendo relevantes y adecuadas en un entorno en constante evolución.

6) Escaneo de vulnerabilidades de verificación

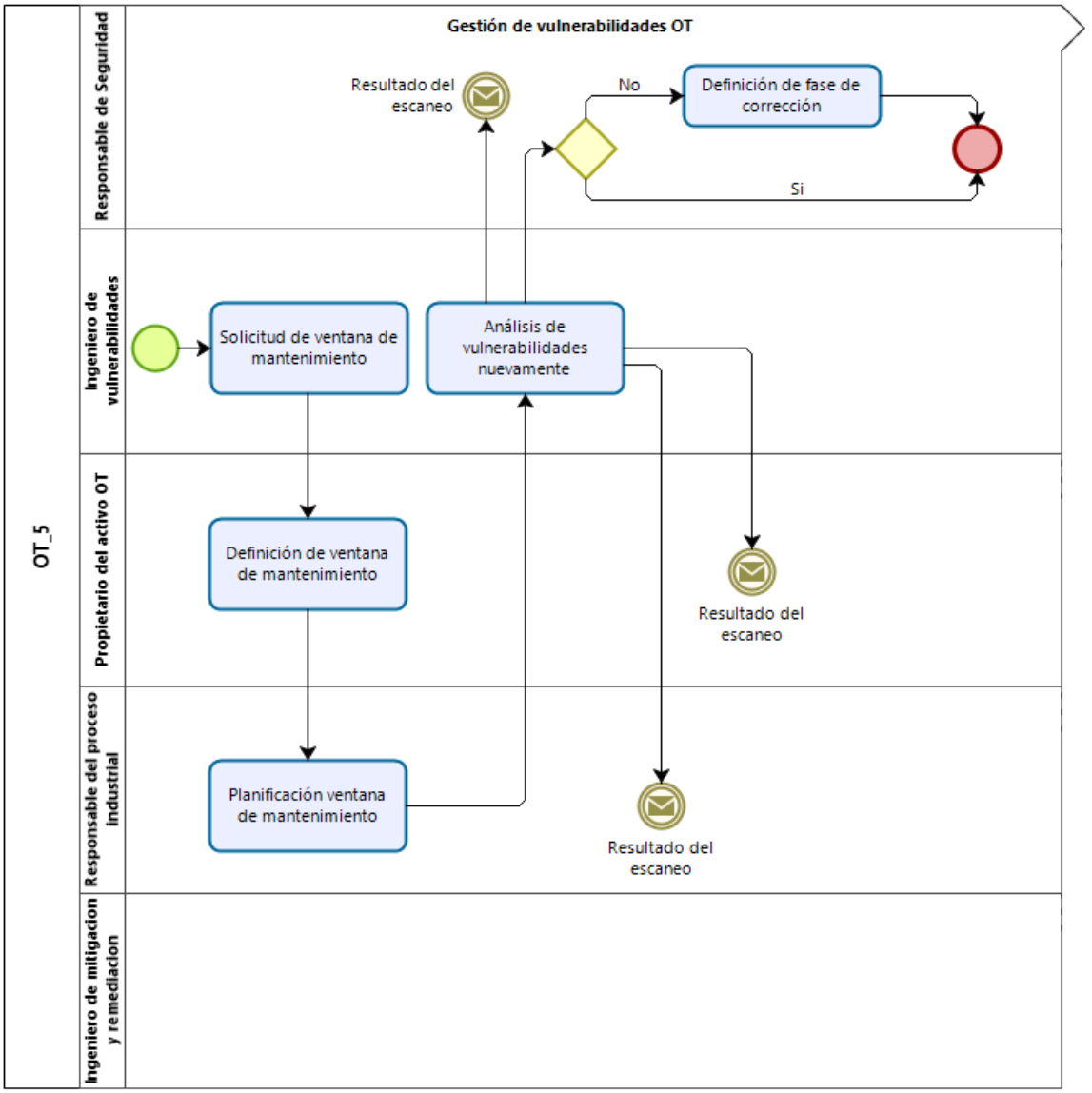

Figura 16 -Escaneo de vulnerabilidades de verificación.

Una vez completada la fase de *"Implementación de contramedidas para mitigar o corregir las vulnerabilidades*", se debe proceder a la validación de las acciones llevadas a cabo. Esta validación se realiza a través de un escaneo de vulnerabilidades específico, que se realiza nuevamente en los activos involucrados durante una ventana de mantenimiento establecida.

Los escaneos de vulnerabilidades en entornos de OT, en comparación con los realizados en IT, presentan una particularidad en cuanto a su demanda y proceso de coordinación. En muchos casos, la implementación de controles compensatorios o contramedidas requiere la validación de múltiples partes interesadas tanto internas como externas, incluyendo proveedores. Esta validación puede llevar tiempo y no se establece una fecha fija con una frecuencia determinada. En su lugar, se planifica de manera gradual a medida que avanza el proceso de validación entre las diferentes partes involucradas.

Este enfoque de planificación flexible permite garantizar la efectividad y la adecuada coordinación de las acciones necesarias para mitigar las vulnerabilidades en entornos OT. A medida que se avanza en el proceso de validación y se obtienen los acuerdos necesarios, se establecen las fechas y frecuencias de los escaneos de vulnerabilidades, asegurando así una implementación eficiente de los controles compensatorios.

Además, se debe tener en cuenta que el escaneo de validación debe realizarse bajo las mismas condiciones de configuración que se establecieron en la fase anterior. Esto garantiza la consistencia en los resultados obtenidos y permite una comparación precisa con los informes generados durante el escaneo inicial. El objetivo es determinar si las acciones implementadas en el plan de remediación cumplen con las metas establecidas y han logrado mitigar de manera efectiva las vulnerabilidades identificadas.

Durante el escaneo de validación, también es importante considerar la posibilidad de riesgos residuales que puedan persistir a pesar de la implementación de las contramedidas. Estos riesgos deben ser cuidadosamente analizados y evaluados para determinar si requieren medidas adicionales o si son aceptables dentro de los límites establecidos por la organización.

La validación del plan de mitigación mediante el escaneo de vulnerabilidades proporciona una visión integral de la efectividad de las acciones implementadas y su impacto en la seguridad de los activos industriales. Permite verificar la adecuada configuración de los sistemas, la correcta aplicación de las contramedidas y la reducción del riesgo en comparación con el estado inicial. Esta validación es un paso fundamental en el proceso de gestión de vulnerabilidades, ya que asegura que las medidas implementadas estén alineadas con los objetivos de seguridad y proporciona una base sólida para la toma de decisiones futuras en la protección del entorno industrial.

Conclusiones

Basado en el trabajo de investigación realizado en este trabajo de tesis de maestría, en cuanto al estado del arte en redes de propósito general, como las redes IT, y su extrapolación al entorno industrial, se determinó que la gestión de vulnerabilidades desempeña un papel fundamental en el ámbito de la ciberseguridad organizacional.

La gestión de vulnerabilidades se ha identificado como una actividad fundamental dentro de los planes y programas de ciberseguridad de las organizaciones, ya que se basa en la evaluación y gestión de riesgos. Aunque no se puede controlar completamente la presencia de amenazas, es posible disminuir el impacto mediante el enfoque en las vulnerabilidades.

Esta gestión de vulnerabilidades realizada con eficacia y eficiencia, permite priorizar la aplicación de contramedidas y asignar recursos de manera adecuada en función de las vulnerabilidades identificadas, lo que a su vez conduce a una reducción efectiva del riesgo. Además, proporciona un mapa claro de las vulnerabilidades presentes en los sistemas industriales y facilita el desarrollo de un plan estratégico para mejorar continuamente la postura de ciberseguridad de la organización.

Es importante destacar que la gestión de vulnerabilidades requiere una comprensión profunda de los activos de la organización, su clasificación y su relación con los procesos industriales. Esta información permite una evaluación precisa del impacto potencial de las vulnerabilidades detectadas y ayuda a establecer un enfoque estratégico para su mitigación. Por tanto, se debe establecer una frecuencia adecuada para las actividades de gestión de vulnerabilidades, lo que garantiza una respuesta oportuna y efectiva ante las amenazas en constante evolución.

En conclusión, la gestión de vulnerabilidades es un componente esencial en la estrategia de ciberseguridad de las organizaciones. Al adoptar un enfoque proactivo y centrado en las vulnerabilidades, las empresas pueden fortalecer su capacidad para proteger sus sistemas industriales y mantener una postura de ciberseguridad sólida en un entorno en constante cambio.

Trabajos a futuro

A partir de las conclusiones obtenidas en este estudio, se pueden plantear varias líneas de investigación futuras relacionadas con la gestión de vulnerabilidades en sistemas industriales. Algunas de estas posibles áreas de investigación son las siguientes:

1. Investigación sobre la aplicación de técnicas avanzadas de análisis de vulnerabilidades en sistemas industriales, como el análisis de penetración o el análisis de código fuente. Esta investigación podría explorar cómo estas técnicas pueden mejorar la eficacia de la gestión de vulnerabilidades en entornos industriales.

2. Estudio sobre la integración de herramientas de gestión de vulnerabilidades con otras soluciones de seguridad, como firewalls y sistemas de detección de intrusiones. Esta investigación podría investigar cómo la integración de estas soluciones puede mejorar la eficacia de la gestión de vulnerabilidades y reducir el riesgo de ataques cibernéticos.

3. Análisis de la efectividad de los procedimientos de gestión de vulnerabilidades en entornos industriales críticos, como la industria de la energía o la industria química. Esta investigación podría evaluar la eficacia de los procedimientos de gestión de vulnerabilidades existentes y proponer mejoras para garantizar una gestión de riesgos más eficaz.

4. Investigación sobre la adaptación de los procesos de gestión de vulnerabilidades a los entornos de sistemas industriales emergentes, como el Internet de las cosas industrial (IIoT). Esta investigación podría explorar cómo los procesos de gestión de vulnerabilidades existentes deben adaptarse para abordar las nuevas amenazas y desafíos de seguridad que plantea el IIoT.

Glosario

El presente glosario tiene como objetivo proporcionar una comprensión clara y concisa de los términos técnicos y especializados utilizados en este trabajo de investigación. Dado que la temática abordada en esta tesis se centra en la gestión de vulnerabilidades en sistemas industriales, es esencial definir estos términos para garantizar una comprensión adecuada de los conceptos presentados.

El glosario incluye una lista de términos técnicos y acrónimos comúnmente utilizados en la literatura técnica y científica, así como sus definiciones correspondientes. Esta sección será de gran ayuda para el lector al momento de leer y comprender los resultados y conclusiones de este trabajo. A continuación, se introducen los términos utilizados en el marco teórico sobre la gestión de riesgos (Incibe - Instituto Nacional de Ciberseguridad, 2015):

- **Activo**: Cualquier elemento de valor para la organización, es decir, cualquier elemento tangible (como hardware) o intangible (por ejemplo, la propiedad intelectual), recurso o la habilidad que tiene valor o sea crítico para la existencia de la organización, y que Por tanto necesita protección (Kowask Bezerra et al., 2021).
- **Amenaza**: Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. En la evolución de las normas este concepto se amplía para denominarse «*suceso*» (Incibe - Instituto Nacional de Ciberseguridad, 2015).
- **Vulnerabilidad**: Una vulnerabilidad se define en la norma ISO 27002 como "Una debilidad de un activo o grupo de activos que puede ser explotado por una o más amenazas" (International Organization for Standardization, 2013).

- **Impacto o consecuencia**: Materialización de una amenaza sobre un activo aprovechando una vulnerabilidad. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo. La consecuencia en las nuevas normas es el resultado de un suceso que afecta a los objetivos (Incibe - Instituto Nacional de Ciberseguridad, 2015).

- **Probabilidad**: Es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento. La frecuencia de ocurrencia implícita se corresponde con la amenaza. Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos). Este término permanece en la evolución de las normas ISO refiriéndose a un suceso en lugar de a una amenaza (Incibe - Instituto Nacional de Ciberseguridad, 2015).

- **Control:** Es cualquier procedimiento administrativo, físico u operacional capaz de tratar los riesgos de la ocurrencia de un incidente de seguridad (Kowask Bezerra et al., 2021).

- **Escaneo de red externo**: Proporciona una visión general de las vulnerabilidades que son visibles desde el exterior de la organización. Este tipo de escaneos puede incluir firewalls, sistemas de detección de intrusos (IDS), así como cualquier otro control de seguridad que se encuentre presente en la arquitectura de la organización. Los resultados del escaneo externo brindan información sobre la correcta configuración de los controles de seguridad.

- **Tecnologías de la información (IT):** se refiere a las herramientas y tecnologías que se utilizan para procesar, almacenar y transmitir información en una organización, incluyendo hardware, software, redes y bases de datos.

- **Tecnologías de operación (OT):** se refiere a las herramientas y tecnologías que se utilizan para controlar, supervisar y optimizar los procesos y sistemas en una organización, incluyendo sistemas de automatización y control industrial.

- **Sistemas industriales:** se refiere a los sistemas y procesos utilizados en la industria para producir bienes o servicios, incluyendo sistemas de control y automatización.

- **Plataformas propietarias:** son sistemas o tecnologías que son propiedad de una empresa en particular y no están disponibles para su uso público o bajo licencia.

- **SCADA:** siglas en inglés de "Supervisory Control And Data Acquisition". Se trata de un sistema de control y supervisión utilizado en la automatización de procesos industriales.

- **PLC:** las siglas en inglés de "Controlador Lógico Programable" (Programmable Logic Controller, en inglés) se refieren a un tipo de dispositivo electrónico utilizado en entornos industriales para controlar y automatizar procesos, máquinas y sistemas.

- **HMI:** las siglas en inglés de "Interfaz Hombre-Máquina" (Human Machine Interface, en inglés) se refieren a un dispositivo o software que permite a los usuarios interactuar con máquinas y sistemas industriales mediante una interfaz gráfica.

- **DCS:** las siglas en inglés de "Sistema de Control Distribuido" (Distributed Control System, en inglés) se refieren a un sistema de control utilizado en entornos industriales que distribuye el control de procesos a través de una red de dispositivos interconectados, como sensores, actuadores y controladores.

- **RTUs:** Las siglas RTU significan "Unidad Terminal Remota". Una RTU es un dispositivo electrónico que se utiliza en sistemas de control industrial para monitorizar y controlar equipos de campo, como bombas, válvulas y motores. Las RTUs son utilizadas para recopilar datos de sensores y enviar comandos a equipos de campo. También pueden servir como puntos de conexión para la comunicación de datos entre equipos de campo y sistemas de control superiores.

- **Sensores:** Un sensor es un dispositivo que detecta y mide cambios en una variable física, como temperatura, presión, humedad, nivel, movimiento, entre otros. Los sensores son ampliamente utilizados en la automatización industrial para medir variables de proceso y proporcionar datos precisos y en tiempo real que se utilizan para el control y monitoreo de procesos.

- **Estaciones de ingeniería:** Las estaciones de ingeniería son sistemas informáticos utilizados por ingenieros y técnicos para diseñar, implementar y mantener sistemas de control industrial. Estas estaciones de trabajo están equipadas con software especializado y herramientas para programar y configurar RTUs, PLCs, HMI y otros dispositivos de automatización industrial.

- **Vector de ataque:** El vector de ataque se refiere al método utilizado por un atacante para penetrar en un sistema o red informática. Es el camino utilizado por el atacante para infiltrarse en el sistema y llevar a cabo sus objetivos malintencionados. Los vectores de ataque pueden incluir la explotación de vulnerabilidades en el software o el hardware, la ingeniería social, la suplantación de identidad, el phishing, entre otros.

- **Hardware genérico:** se refiere a dispositivos de hardware que son producidos por varias empresas diferentes y no están limitados a una sola marca o modelo.

- **Sistemas operativos:** es el software que se encarga de administrar los recursos de hardware y software de un ordenador y proporciona servicios a las aplicaciones.

- **Industria 4.0:** Es el término utilizado para describir la cuarta revolución industrial, que se basa en la digitalización y la automatización de los procesos industriales.

- **Continuidad del proceso industrial:** se refiere a la capacidad de mantener el proceso de producción en funcionamiento sin interrupciones o fallos.

- **Experiencia de usuario:** es la percepción que tiene un usuario sobre la facilidad de uso y eficacia de un sistema o aplicación.

- **Riesgos:** son eventos o circunstancias que pueden tener un impacto negativo en la organización, incluyendo pérdidas financieras, daños a la reputación, interrupciones del negocio o lesiones a las personas.

- **Infraestructura vulnerable:** se refiere a los sistemas o componentes que son susceptibles de ser explotados o atacados.

- **Medidas preventivas:** son las acciones que se toman para evitar o minimizar el impacto de un riesgo.

- **Gestión de vulnerabilidades:** es el proceso de identificación, análisis y mitigación de vulnerabilidades en un sistema o infraestructura.
- **Contramedidas:** soluciones para mitigar o corregir las vulnerabilidades identificadas
- **Parches:** actualizaciones de software que solucionan vulnerabilidades conocidas
- **Controles compensatorios:** medidas alternativas para mitigar o eliminar el riesgo sin corregir la vulnerabilidad.
- **Firmware**: Es un software que se encuentra programado en un dispositivo de hardware, el cual proporciona instrucciones de bajo nivel al dispositivo y lo controla. Es utilizado en una variedad de dispositivos, desde electrodomésticos hasta sistemas informáticos, y debe ser actualizado periódicamente para corregir errores y mejorar su funcionalidad.
- **Protocolo OPC**: Es un protocolo de comunicación utilizado en la automatización industrial para intercambiar información entre dispositivos y aplicaciones. OPC significa "OLE for Process Control" y utiliza la tecnología de objetos COM (Component Object Model) de Microsoft para proporcionar una interfaz entre los sistemas de control y las aplicaciones de software.
- **Protocolo inseguro**: Se refiere a un protocolo de comunicación que presenta deficiencias en su diseño o implementación que pueden ser explotadas por los atacantes para comprometer la seguridad de los sistemas y redes que lo utilizan. Los protocolos inseguros son una preocupación importante en la seguridad de la información y se requiere que sean actualizados o reemplazados para garantizar su seguridad.
- **Tecnología DCOM**: Es una tecnología de Microsoft que permite la comunicación entre procesos en sistemas operativos Windows. DCOM significa "Distributed Component Object Model" y se utiliza para permitir que los componentes de software se comuniquen entre sí en una red. Sin embargo, debido a sus deficiencias de seguridad, DCOM se considera obsoleto y se recomienda su reemplazo por tecnologías más seguras.

- **Escaneo de red interno:** Proporciona una visión general de las vulnerabilidades que son visibles desde la red local, teniendo en cuenta los controles de seguridad presentes en la arquitectura de la organización. Al realizar un escaneo interno de cada componente de una arquitectura, los resultados pueden proporcionar información sobre el grado de seguridad de cada capa defensa en profundidad[12]

[12] Mediante este enfoque se pretende implementar una serie de mecanismos y controles tecnológicos heterogéneos de forma selectiva para proteger la confidencialidad, integridad y disponibilidad de la red y los datos que ésta contiene. Si bien ninguna tecnología o control individual puede contener todas las amenazas y ataques, juntas brindan mitigaciones frente a una amplia variedad de estas, al tiempo que incorporan diversidad y redundancia en caso de que algún mecanismo o control particular fallara (Center for Internet Security, 2022).

Referencias bibliográficas y bibliografía

Center for Internet Security. (2022). Election Security Spotlight – Defense in Depth (DiD). https://www.cisecurity.org/insights/spotlight/cybersecurity-spotlight-defense-in-depth-did

Committee of Sponsoring Organizations of the Treadway Commission. (2015). Guidance.

Dirección Nacional - Interoperabilidad, S. de la I. e I. (2020). Guía para la gestión de riesgos de seguridad de la información. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Divino, B. V. (2018). Evaluación y gestión de vulnerabilidades: Cómo sobrevivir en el mundo de los ciberataques.

G. Stoneburner, C. Hayden, and A. F. (2004). Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A.

Gobierno de España – ADMINISTRACIÓN ELECTRÓNICA. (2015). MAGERIT V3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Incibe - Instituto Nacional de Ciberseguridad. (2015). Gestión de riesgos - Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_gestion_riesgos_metad.pdf

International Organization for Standardization. (2013). ISO/IEC 27002. https://www.iso27000.es/iso27002.html

International Organization for Standarization. (2009). ISO 31000:2009 Risk management – Principles and guidelines.

International Organization for Standarization. (2011). ISO 27005: Information technology - Security techniques - Information security risk management.

International Organization for Standarization. (2013). ISO/IEC 27001. Information technology. Security techniques. Information security management systems. Requirements.

International Organization for Standarization. (2018). NTC-ISO 31000. Risk Management, Principles and Guidelines. NTC-ISO 31000:2018.

International Society of Automation. (2007). Assessing the Cybersecurity of New or Existing IACS Systems - ANSI/ISA–62443-1-1.

International Society of Automation. (2017). Using the ISA/IEC 62443 Standard to Secure Your Control Systems.

International Society of Automation. (2020). Assessing the Cybersecurity of New or Existing IACS Systems - ANSI/ISA 62443-3-3.

Kowask Bezerra, E., Alcántara Lima, F., Cesar Motta, A., & Boca Piccolini, J. D. (2021). Gestión del riesgo de las TI NTC 27005.M.

Whitman and H. Mattord. (2011). Principles of Information Security, 4th ed. Course Technology.

National Institute of Standards and Technology. (2012). Guide for conducting risk assessment, Computer Security Division Information Technology Laboratory.

Palmaers, T. (2021). Implementing a Vulnerability Management Process.

¿Qué es la Industria 4.0? | Argentina.gob.ar. (n.d.). Retrieved September 7, 2021, from https://www.argentina.gob.ar/produccion/planargentina40/industria-4-0

Real Academia Española. (2021). ad hoc | Definición | Diccionario de la lengua española | RAE - ASALE. https://dle.rae.es/ad%20hoc

Romero, M. I., Grace, C., Figueroa, L., Denisse, M., Vera, S., José, N., Álava, E., Galo, C., Parrales, R., Christian, A., Álava, J., Ángel, M., Murillo Quimiz, L., Adriana, M., & Merino, C. (2018). INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES.

SYNNEX Westcon-Comstor. (2020). Gestión de vulnerabilidades: ¿qué es y cómo ponerla en práctica?
https://digital.la.synnex.com/gestion-de-vulnerabilidades-que-es-y-como-ponerla-en-practica

Technology National Institute of Standards and Technology. (2019). NIST Cybersecurity Framework. https://www.nist.gov/cyberframework

Tyson, M., & Bryan L., S. (2011). Cybersecurity for Industrial Control Systems.

Wiley, J. (2008). Vulnerability management.

Anexo

El presente trabajo de investigación ha sido el resultado de un esfuerzo arduo y dedicado por parte del autor, en el que se han abordado diferentes aspectos relacionados con el tema de estudio. Durante el proceso, se han recopilado datos, se han realizado análisis y se han extraído conclusiones significativas que han permitido avanzar en el conocimiento y la comprensión de la problemática tratada.

Sin embargo, es importante destacar que este trabajo no habría sido posible sin el apoyo de diferentes fuentes de información y herramientas utilizadas en su elaboración. Es por ello que en esta sección de anexos se presentan una serie de documentos, imágenes y materiales complementarios que han sido de utilidad para el desarrollo del trabajo y que se consideran relevantes para su comprensión y contextualización.

Los anexos incluidos en este trabajo no solo ofrecen una ampliación de la información proporcionada en el cuerpo principal de la tesis, sino que también brindan al lector la oportunidad de profundizar en ciertos aspectos específicos que puedan resultar de su interés. Se espera que la inclusión de estos materiales adicionales enriquezca la experiencia del lector y contribuya a una mejor comprensión del tema tratado en este trabajo.

Gestión de riesgos

Las actividades cuyo objetivo es mantener el riesgo por debajo del umbral fijado se engloban en lo que se denomina “Gestión de riesgos”. Las organizaciones que decidan gestionar el riesgo para su actividad deberán realizar dos grandes tareas:

- **Análisis de riesgo:** Que consiste en averiguar el nivel de riesgo que la empresa está soportando. Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos.

- **Tratamiento de los riesgos:** Para aquellos riesgos cuyo nivel está por encima del umbral deseado la empresa debe decidir cuál es el mejor tratamiento que permita disminuirlos. Esta decisión siempre ha de pasar un filtro económico donde el costo del tratamiento, o costo de protección, no supere el costo de riesgo disminuido.

Por tanto, la Gestión de riesgos se puede calcular con la siguiente fórmula:

GESTIÓN DE RIESGOS = ANÁLISIS DE RIESGOS + TRATAMIENTO DE RIESGOS

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo con la estrategia de la organización. Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo.

Para el tratamiento de riesgos las empresas cuentan, entre otras, con las siguientes opciones:

- **Evitar o eliminar el riesgo**: Por ejemplo, sustituyendo el activo por otro que no se vea afectado por la amenaza o eliminando la actividad que lo produce.
- **Reducirlo o mitigarlo:** Tomando las medidas oportunas para que el nivel de riesgo se sitúe por debajo del umbral. Para conseguirlo se puede:
    - Reducir la probabilidad o frecuencia de ocurrencia: tomando, por ejemplo, medidas preventivas.
    - Reducir el impacto de la amenaza o acotar el impacto, estableciendo por ejemplo controles y revisando el funcionamiento de las medidas preventivas
- **Transferirlo, compartirlo o asignarlo a terceros:** En ocasiones la empresa no tiene la capacidad de tratamiento y precisa la contratación de un tercero con capacidad para reducir y gestionar el riesgo dejándolo por debajo del umbral.

- **Aceptarlo:** Se asume el riesgo, bien porque está debajo del umbral aceptable de riesgo bien en situaciones en las que los costos de su tratamiento son elevados y aun siendo riesgos de impacto alto su probabilidad de ocurrencia es baja o porque aun a pesar del riesgo la organización no quiere dejar de aprovechar la oportunidad que para su negocio supone esa actividad arriesgada.

Gestión de riesgos de seguridad de la información

La seguridad de la información generalmente está enfocada hacia los sistemas de Tecnologías de Información, incluye la seguridad tanto física como operacional y organizacional del sistema de información. A continuación, se describen los principios que conforman la seguridad de la información CIA[13] (M. Whitman and H. Mattord, 2011):

- **Integridad**: es la garantía de la exactitud y completitud de la información y los métodos de su procesamiento, se debe asegurar que la información puede ser lo suficientemente precisa para su propósito. Este principio representa uno de los principales indicadores de seguridad de la información. La integridad de la información, no se basa solo en que el dato sea correcto, sino que, además, se pueda confiar en él (Dirección Nacional - Interoperabilidad, 2020).
- **Confidencialidad**: principio de seguridad que genera el requisito de protección contra intentos deliberados o accidentales para realizar lectura de datos no autorizados. La confidencialidad abarca los datos en el almacenamiento, durante el proceso y mientras están en tránsito (G. Stoneburner, C. Hayden, 2004).

  Es la garantía de que la información se comparte solo entre personas u organizaciones autorizadas. La violación de este principio se puede dar cuando los datos no se manejan de manera adecuada (Dirección Nacional - Interoperabilidad, 2020). Para esto, se tienen métodos de aseguramiento como tipos de cifrado: simétrico (una clave secreta, se aplica al texto de un mensaje para cambiar su contenido) o asimétrico (un par de claves, una

[13] https://www.computerweekly.com/es/opinion/Que-es-la-triada-de-la-CIA

pública disponible para cualquier persona que quiera enviar un mensaje y una privada solo para la persona que la conoce)

- **Disponibilidad**: principio de seguridad que declara que los usuarios autorizados tienen acceso a la información cuando lo requieran y de que el sistema es capaz de recuperarse rápida y completamente en caso de ocurrir un desastre. En este principio se consideran aspectos como: tolerancia a fallos, recuperación, redundancia, entre otros. Este principio genera el requisito de la protección contra algún modo de causar una denegación de servicios o de datos (G. Stoneburner, C. Hayden, 2004).

Riesgos de vulnerabilidades en entornos industriales

Los entornos industriales son cada vez más complejos, con una gran variedad de sistemas y dispositivos interconectados que facilitan la automatización de procesos y la toma de decisiones. Sin embargo, esta complejidad también introduce una serie de riesgos de vulnerabilidades que pueden poner en peligro la seguridad y la integridad de los sistemas y datos críticos.

Los riesgos de vulnerabilidades en entornos industriales son múltiples y variados, y pueden representar una amenaza importante para la continuidad de las operaciones y la seguridad de la empresa. A continuación, profundizaremos en algunos de los riesgos más comunes.

- Accesos no autorizados a sistemas y datos críticos: Uno de los mayores riesgos en cualquier entorno industrial es el acceso no autorizado a sistemas y datos críticos. Esto puede ocurrir por medio de ataques cibernéticos o por la mala gestión de contraseñas y permisos. Los resultados pueden ser devastadores para la empresa, incluyendo la pérdida de propiedad intelectual, la exposición de información confidencial y la interrupción de las operaciones.

- Interrupciones en el suministro eléctrico o de otros recursos: Las interrupciones en el suministro eléctrico o de otros recursos también son un riesgo importante en los entornos industriales. Los cortes de energía pueden detener las operaciones críticas y causar la pérdida de producción y beneficios. Además, las interrupciones en el suministro de agua, gas u otros recursos también pueden afectar las operaciones.
- Fugas de información confidencial: En los entornos industriales, la información confidencial es un recurso valioso que debe ser protegido adecuadamente. Las fugas de información pueden ocurrir por múltiples razones, como por ejemplo por el robo de dispositivos móviles o por el mal uso de contraseñas. La exposición de información confidencial puede ser devastadora para la empresa, especialmente si se trata de datos de clientes o de propiedad intelectual.
- Robos de propiedad intelectual o industrial: El robo de propiedad intelectual o industrial es un riesgo real en los entornos industriales. Esto puede incluir la copia de diseños, patentes o fórmulas secretas, y puede ser causado por los propios empleados o por competidores deshonestos. Los robos de propiedad intelectual o industrial pueden tener un impacto significativo en la competitividad de la empresa y en su capacidad para innovar.
- Daños a equipos y sistemas críticos: Los equipos y sistemas críticos son esenciales para las operaciones industriales. Cualquier daño a estos equipos y sistemas puede tener un impacto significativo en la capacidad de la empresa para producir y cumplir con sus compromisos. Los riesgos incluyen fallas de hardware, errores de software y fallos en la infraestructura de red.

En consecuencia, es vital que las empresas industriales implementen medidas adecuadas para la gestión de riesgos, incluyendo la identificación y evaluación de los riesgos, la implementación de medidas preventivas y correctivas y la revisión periódica del plan de gestión de riesgos. De esta manera, se pueden minimizar los riesgos y proteger adecuadamente a la empresa contra cualquier amenaza potencial.

Gestión de riesgos en entornos industriales

La gestión de riesgos en entornos industriales es una actividad esencial para garantizar la seguridad y la estabilidad de los sistemas y procesos críticos. Esta gestión implica la identificación, análisis, evaluación y mitigación de los riesgos potenciales que pueden afectar a la operatividad y el rendimiento del entorno.

Para identificar los riesgos potenciales en un entorno industrial, se pueden realizar diferentes técnicas, como la observación, entrevistas, análisis de datos históricos y análisis de documentos. Es importante considerar todos los aspectos del entorno, como la infraestructura, los procesos, los recursos humanos y las tecnologías utilizadas.

Una vez identificados los riesgos, es necesario realizar un análisis detallado de cada uno de ellos, evaluando su probabilidad de ocurrencia y su impacto potencial. Esta evaluación permitirá establecer la prioridad de los riesgos y determinar las medidas de mitigación necesarias para minimizar su impacto.

Al evaluar los riesgos, es importante considerar la interdependencia entre los riesgos y cómo pueden afectarse entre sí. De esta manera, se podrán establecer medidas de mitigación integrales y efectivas que aborden múltiples riesgos al mismo tiempo.

Luego de establecer las medidas de mitigación necesarias, es fundamental implementarlas de manera efectiva. Esto puede incluir la implementación de controles de seguridad adicionales, el fortalecimiento de la infraestructura y tecnologías utilizadas, y la capacitación del personal para la detección y respuesta a riesgos.

Finalmente, es importante monitorear y revisar continuamente el entorno industrial para detectar posibles riesgos y evaluar la efectividad de las medidas de mitigación implementadas. Este monitoreo debe ser una actividad regular y constante, que permita ajustar las medidas de mitigación en función de los cambios en el entorno y la evolución de los riesgos identificados.

Gestión de vulnerabilidades en entornos industriales

La gestión de vulnerabilidades en entornos industriales es una tarea crítica para garantizar la seguridad de los sistemas y procesos utilizados en la industria. Las vulnerabilidades son fallos o debilidades en los sistemas que pueden ser explotados por atacantes malintencionados para comprometer la seguridad del sistema, y pueden ser introducidos en los sistemas de muchas maneras, incluyendo errores de diseño, configuraciones inadecuadas, software malicioso y errores humanos.

Para gestionar adecuadamente las vulnerabilidades en entornos industriales, es necesario seguir un enfoque sistemático que comience por la identificación de las vulnerabilidades presentes en el sistema, seguido de una evaluación del riesgo asociado a cada una de ellas. Una vez identificadas y evaluadas las vulnerabilidades, se pueden aplicar medidas de mitigación apropiadas para minimizar el riesgo.

Las medidas de mitigación pueden incluir la aplicación de parches y actualizaciones de software, la implementación de controles de acceso físico y lógico, la implementación de firewalls y otros sistemas de seguridad de red, y la adopción de políticas y procedimientos de seguridad robustos. Es importante destacar que la gestión de vulnerabilidades debe ser un proceso continuo y evolutivo, ya que las amenazas y los riesgos cambian con el tiempo, y nuevas vulnerabilidades pueden surgir en cualquier momento.

Además, la gestión de vulnerabilidades debe ser parte de un enfoque más amplio de seguridad de la información en la industria, que incluya la identificación de activos críticos, la evaluación de riesgos y la implementación de controles de seguridad adecuados en todos los aspectos del entorno industrial. En última instancia, la gestión de vulnerabilidades en entornos industriales es una tarea crítica para garantizar la seguridad de los sistemas y procesos industriales, y debe ser una prioridad para cualquier organización que opere en este entorno.

Lecciones aprendidas

Análisis de dos ataques cibernéticos en entornos industriales

Existen varios casos de ataques reales a entornos industriales en todo el mundo, algunos de los cuales han tenido graves consecuencias. A continuación se describe uno de los casos más destacados:

Stuxnet: El malware que cambió la ciberseguridad industrial

En 2010 se descubrió Stuxnet, un gusano informático diseñado para atacar sistemas de control industrial específicos. Este ataque fue uno de los primeros en su tipo y demostró la capacidad de los atacantes para infiltrarse en sistemas industriales altamente protegidos. El gusano se propagó a través de dispositivos USB y explotó una vulnerabilidad en el software de control industrial utilizado por las centrifugadoras de enriquecimiento de uranio en la planta nuclear de Natanz en Irán. Una vez dentro del sistema, Stuxnet controló las centrifugadoras y las hizo girar a velocidades anormales, lo que causó daños significativos y redujo la capacidad de enriquecimiento de uranio de Irán. Se cree que el ataque fue desarrollado por un equipo conjunto de Estados Unidos e Israel como parte de una operación cibernética encubierta. Este ataque demostró la capacidad de los atacantes para causar daños físicos y reales en instalaciones críticas a través de la explotación de vulnerabilidades de seguridad en sistemas de control industrial.

Industroyer: Riesgo la infraestructura crítica

Otro caso de ataque real en entornos industriales ocurrió en 2017 en Ucrania, donde los sistemas de control industrial de la central eléctrica de Prykarpattya fueron atacados por un malware conocido como "Crash Override" o "Industroyer". Este malware logró tomar control de los sistemas de control industrial y causar un apagón que afectó a más de 225,000 personas en Ucrania. Fue la primera vez que se utilizó un malware específicamente diseñado para atacar sistemas de control industrial en un ataque real y tuvo un impacto significativo en la infraestructura crítica del país.

Triton: Su impacto en la seguridad de los sistemas de control

Un ejemplo de otro malware que ha sido utilizado para atacar sistemas de control industrial es el Triton (también conocido como Trisis).
Triton es un malware altamente sofisticado diseñado para atacar sistemas de control industrial (ICS). El objetivo de este malware es manipular los procesos de los sistemas de control industrial con el fin de causar daños físicos. Fue identificado por primera vez en 2017 cuando se utilizó para atacar una planta petroquímica en Oriente Medio.

Triton se instala en los sistemas de control industrial mediante la explotación de vulnerabilidades en los protocolos de comunicación de estos sistemas, lo que le permite obtener acceso a los controladores lógicos programables (PLC) utilizados en los procesos industriales. Una vez instalado en el sistema, Triton se comunica con los PLC y realiza una serie de acciones maliciosas. Por ejemplo, puede modificar el código de control que ejecutan los PLC, lo que puede provocar fallos en el sistema y, en última instancia, daños físicos a los equipos y a la infraestructura.

Lo que hace que Triton sea particularmente peligroso es que se dirige a los sistemas de seguridad que se utilizan para proteger los sistemas de control industrial. Por ejemplo, Triton puede desactivar los sistemas de seguridad que se utilizan para detener los procesos de manera segura en caso de emergencia. Al hacerlo, Triton puede poner en peligro la seguridad de los trabajadores y causar daños graves a los equipos y a la infraestructura.

La complejidad y sofisticación de Triton sugieren que fue desarrollado por un actor estatal o un grupo de hackers altamente financiado y experimentado. Es importante destacar que Triton no es un malware de "robo de datos", sino un malware diseñado específicamente para causar daños físicos en los sistemas de control industrial. La naturaleza altamente destructiva de este malware significa que las organizaciones industriales deben tomar medidas para proteger sus sistemas de control contra este tipo de amenaza.

Categorías de roles de trabajo del Marco NICE

El NICE Framework define varios roles y responsabilidades en el campo de la ciberseguridad. A continuación, se presentan algunos de los roles clave:

- Analista de ciberseguridad: Se encarga de recopilar y analizar datos de seguridad, evaluar riesgos y amenazas, y desarrollar estrategias para proteger los sistemas y datos de la organización.
- Administrador de sistemas de seguridad: Responsable de implementar y administrar sistemas y herramientas de seguridad, como firewalls, sistemas de detección de intrusiones y sistemas de prevención de pérdida de datos.
- Investigador forense digital: Encargado de recolectar y analizar evidencia digital en caso de incidentes de seguridad, realizar investigaciones de incidentes y colaborar con las autoridades legales en la resolución de delitos cibernéticos.
- Ingeniero de redes seguras: Diseña, implementa y mantiene redes seguras, utilizando tecnologías y prácticas de seguridad para proteger la infraestructura de red y los sistemas de la organización.
- Especialista en cumplimiento y auditoría de seguridad: Se asegura de que la organización cumpla con las regulaciones y estándares de seguridad, llevando a cabo auditorías internas y externas, evaluando el cumplimiento y recomendando mejoras.
- Experto en respuesta a incidentes: Responde de manera rápida y eficiente a los incidentes de seguridad, investiga las causas raíz, mitiga el impacto y realiza acciones correctivas para evitar futuros incidentes.
- Desarrollador de aplicaciones seguras: Integra prácticas de seguridad en el ciclo de desarrollo de software, identificando y resolviendo vulnerabilidades en las aplicaciones para protegerlas contra ataques y brechas de seguridad.