UNIVERSIDAD CENTRAL

VICERRECTORÍA ACADÉMICA

ESCUELA DE CIENCIAS DE LA INGENIERÍA

AUTOMATIZACIÓN DEL PROCESO DE DETECCIÓN Y CORRECCIÓN DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DEL INS

MODALIDAD DE TESIS PARA OPTAR POR EL GRADO DE LICENCIATURA EN INGENIERÍA INFORMÁTICA
CON ÉNFASIS EN GERENCIA INFORMATICA

CRISTIAN JIMENEZ PEÑARANDA

TUUTOR: LIC. RODRIGO GUERRERO JIMENEZ

SEDE CENTRAL
ABRIL, 2025

Contenido

Tablas

Figuras

Dedicatoria

Dedico este trabajo a mi esposa María Fernanda y a mis hijos Valeria, Marypaz y Gabriel, por todo su apoyo y su amor, por ser el motor de mi vida y mi motivación diaria para ser mejor, por hacerme el camino más fácil y estar siempre ahí.

Los amo.

Agradecimiento

Agradezco a la vida, por traerme a este momento y hacerlo en compañía de los seres que amo, mi esposa y mis hijos, sin su apoyo y aliento no hubiera sido posible, a mi esposa por las horas de espera y la paciencia, por las noches sin despedida al estar en clases y las semanas de estrés y cansancio en las que siempre tuvo una palabra de aliento y fuerza, a mis hijos por sus ayudas y por el apoyo, porque cuando ocupé de su guía y sus conocimientos tecnológicos estuvieron conmigo siempre, es una bendición para mi tenerlos.

Al profesor Ing Rodrigo Guerrero Jiménez, mi tutor, por su paciencia, su guía y su disposición de ayuda y consejo siempre, por exigirme al máximo y hacerme un mejor profesional con más conocimiento del que tenía al inicio, no pude haber tenido mejor guía en este proceso.

A mis compañeros de trabajo por su espíritu de colaboración y por brindarme siempre la mano, por contestar mis preguntas y brindarme tiempo del que no tenían para avanzar en mi investigación.

Gracias a todos de todo corazón, sin ustedes no hubiera sido posible.

Resumen Ejecutivo

Esta investigación abordó una propuesta para automatizar los procesos que forman parte de la detección y corrección de vulnerabilidades en el INS, y se enfocó en identificar y conocer el proceso actual, con el fin de encontrar los puntos necesarios de mejora y la utilización de recurso humano, tecnológico y económico.

El problema se centró en ofrecer una alternativa viable de automatización del proceso total que pueda ser implementada en un futuro cercano, eliminando los procesos actuales que son manuales y optimizando de esta forma el uso de recurso humano y tiempos de atención, así como la implementación de soluciones inmediatas con las posibilidades con las que se contaba en el INS.

Los objetivos se concentraron en identificar y entender el proceso actual, investigar las posibilidades existentes en el mercado y que puedan integrarse con las herramientas actuales, automatizar procesos relacionados a la seguridad tecnológica institucional ligados a la corrección de vulnerabilidades y presentar una propuesta que pueda ser implementada en el tiempo. Este estudio utilizó una metodología mixta, pues la calidad del producto final en este caso resulta tan importante como las cantidades de atenciones, de ahorro en tiempo, dinero y de gestión de recursos humanos que intervienen en todo el proceso, para esto se utilizaron encuestas, entrevistas, revisión de documentación y se logró la implementación de las actualizaciones automatizadas en los servidores del ambiente de desarrollo, como parte de las pruebas realizadas.

La propuesta se basó en la automatización total del proceso integrando las diferentes herramientas ya existentes para no solo garantizar la detección y corrección adecuadas, sino también el monitoreo y seguimiento del proceso.

CAPÍTULO 1: PROBLEMA

Problema principal

La coyuntura actual de las empresas, impulsada entre otras cosas por el giro que representó la pandemia de COVID-19, y al incremento de la virtualidad, tanto a nivel laboral como comercial, ha generado un entorno donde la seguridad informática se ha convertido en un aspecto fundamental. Este cambio estructural ha destacado la necesidad de proteger los sistemas tecnológicos como un pilar esencial para garantizar la continuidad operativa y la confianza de los clientes. En este contexto, la detección y corrección oportuna de vulnerabilidades en la infraestructura tecnológica juega un rol preponderante para proteger a las organizaciones contra amenazas tanto externas como internas que podrían comprometer su operación y, por ende, su reputación.

A nivel global, la amenaza de los ciberataques ha alcanzado proporciones alarmantes. De acuerdo con el sitio web de Microsoft, en su informe de protección digital del año 2024, sus clientes se enfrentan cada día a más de 600 millones de ataques cibernéticos. Estas amenazas incluyen desde ramsonware y phishing, hasta ataques de identidad, siendo perpetradas tanto por ciberdelincuentes como por estados-nación. (Microsoft, 2024)

Ejemplos recientes de ciberataques de alto impacto subrayan la diversidad de las organizaciones afectadas. Entre los incidentes más destacados de este año se encuentran:

- Ataque a los sistemas corporativos de Microsoft (enero de 2024)
- La eliminación de 2 petabytes de datos del Centro de Investigación Espacial de Rusia por hacktivistas pro-ucranianos (enero 2024)
- Vulnerabilidades zero-day explotadas en Ivanti VPN (enero 2024)

- El ciberataque a Change Healthcare expone datos de pacientes en Estados Unidos (febrero 2024)
- Ramsomware dirigido a las elecciones en EE.UU.
- Más de 140 ciberataques relacionados con los Juegos Olímpicos.
- Desmantelamiento de computadoras zombies por parte del FBI (Mundial, 2024)

Estos incidentes demuestran que los ciberataques no están limitados a entidades financieras o de seguridad, sino que abarcan diversos sectores. Por ello, la detección y corrección oportuna de vulnerabilidades es crucial para cualquier organización, independientemente de su campo de acción.

En el ámbito regional, las estadísticas también reflejan la gravedad del problema. Un estudio realizado por la empresa Karspersky titulado “Panorama de Amenazas 2024” reveló que en América Latina se bloquearon más de 1.1 billones de ataques de malware entre junio de 2023 y julio de 2024. Esto equivale a 2.2 millones de ataques por minuto. (Karspersky, 2024). En Costa Rica, específicamente, se registraron 2289 ataques de ransomware en el mismo período, lo que pone de manifiesto la magnitud de esta problemática en el país. Además, diversas instituciones gubernamentales han sido víctimas de ciberataques, entre ellas:

- El Ministerio de Hacienda
- La Caja Costarricense del Seguro Social (CCSS)
- El Ministerio de Obras Públicas y Transportes (MOPT)
- RECOPE

Estos casos evidencian la urgencia de fortalecer las medidas de seguridad en todos los niveles, especialmente en el sector público, donde las consecuencias de un ciberataque pueden ser particularmente devastadoras.

Con el crecimiento constante de la tecnología y su integración en casi todos los aspectos de la vida moderna, las infraestructuras tecnológicas (redes, servidores, bases de datos, etc.) están cada vez más expuestas a riesgos de seguridad. En este sentido el Instituto Nacional de Seguros (INS) en Costa Rica reporta anualmente un promedio de 2283 vulnerabilidades, incluyendo alertas espontáneas relacionadas con vulnerabilidades “zero day”. Estas representan un promedio de 240 vulnerabilidades en un período de tres meses. Ante esta situación, la automatización de procedimientos para la detección y corrección de vulnerabilidades se convierte en una prioridad estratégica. La ausencia de estos procedimientos no solo expone a las empresas a pérdidas económicas y reputacionales, sino también pone en riesgo a sus usuarios, clientes y socios, quienes dependen de la tecnología para sus operaciones diarias.

Pregunta de investigación

¿Cómo puede implementarse un modelo automatizado que permita optimizar la detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS) para mejorar la seguridad y minimizar el riesgo de ciberataques?

Objetivo general

Proponer un modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS) con el propósito de optimizar los procesos de seguridad y minimizar los riesgos asociados a los ciberataques,

mediante el análisis de mejores prácticas, herramientas tecnológicas y estándares internacionales de ciberseguridad.

Objetivos específicos

1. Examinar los procesos actuales utilizados por el departamento de Operaciones y Soporte Técnico para identificar las oportunidades de mejora que permitan optimizar la detección y corrección de vulnerabilidades mediante un diagnóstico detallado de la situación actual.
2. Identificar los requerimientos y especificaciones técnicas necesarias para desarrollar un modelo automatizado que garantice la detección y corrección de vulnerabilidades, mediante la consulta de estándares internacionales y mejores prácticas de seguridad informática.
3. Elaborar una propuesta de automatización de procesos que permita la integración de metodologías ágiles y herramientas tecnológicas avanzadas, con el fin de mejorar la eficiencia en la detección y corrección de vulnerabilidades en la infraestructura del INS.

Justificación

En la actualidad, las organizaciones se enfrentan a un entorno digital cada vez más complejo, donde la tecnología es el eje central de sus operaciones y la información es uno de sus activos más valiosos. Sin embargo, con la digitalización, también han surgido amenazas cibernéticas cada vez más sofisticadas que representan riesgos significativos para la seguridad de la información y la continuidad de los servicios. El Instituto Nacional de Seguros (INS), como entidad pública encargada de gestionar seguros y servicios financieros, no está exento de estos desafíos. De hecho, debido a la naturaleza crítica de los servicios que ofrece, es esencial que la

infraestructura tecnológica del INS esté protegida contra las vulnerabilidades que puedan ser explotadas por ciberdelincuentes.

Como ya fue definido previamente, la presente investigación tiene como objetivo diseñar un modelo automatizado que optimice la detección y corrección de vulnerabilidades en la infraestructura tecnológica del INS, con el fin de mejorar la seguridad de sus sistemas y minimizar los riesgos asociados a los ciberataques. La implementación de un modelo de este tipo no solo garantizaría la protección de datos sensibles y las operaciones de la Institución, sino que también mejoraría la resiliencia del INS frente a posibles ataques cibernéticos. Para lograr este objetivo, se llevará a cabo un análisis exhaustivo de las mejores prácticas, herramientas tecnológicas y estándares internacionales de ciberseguridad, con el fin de diseñar un modelo que se ajuste a las necesidades y particularidades del INS.

En este sentido el Instituto Nacional de Seguros, como entidad pública dedicada a la gestión de seguros y servicios financieros, se enfrenta a una serie de retos relacionados con la seguridad de su infraestructura tecnológica. El INS gestiona grandes volúmenes de datos sensibles, como información personal y financiera de sus clientes, así como transacciones críticas que son esenciales para el funcionamiento de la Institución. Cualquier vulnerabilidad en su infraestructura tecnológica puede ser explotada por ciberdelincuentes, lo que pone en riesgo la confidencialidad, la integridad y la disponibilidad de la información, así como la continuidad de los servicios prestados a sus clientes.

El principal problema que enfrenta el INS en términos de seguridad es la detección y corrección de vulnerabilidades. Aunque existen diversas herramientas y tecnologías disponibles para identificar estas vulnerabilidades, muchas de ellas no son lo suficientemente efectivas para detectar amenazas en tiempo real o para corregirlas de manera automatizada y eficiente. Esto

puede generar situaciones en las que las vulnerabilidades no se identifican hasta que ya ha ocurrido un ataque, lo que agrava las consecuencias del incidente y pone en riesgo la estabilidad de los sistemas tecnológicos del INS.

Además, la gestión manual de las vulnerabilidades puede resultar un proceso lento y propenso a errores, lo que aumenta la probabilidad de que un atacante pueda explotar una vulnerabilidad de que sea corregida. Por esta razón, es necesario desarrollar un modelo automatizado que permita detectar y corregir vulnerabilidades de manera muy rápida y precisa, reduciendo la dependencia de la intervención humana y optimizando los recursos disponibles para mejorar la seguridad del INS.

La implementación de un modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológica del INS es de vital importancia por varias razones. En primer lugar, un modelo de este tipo permitiría a la Institución identificar y corregir vulnerabilidades de manera proactiva, antes de que los ciberdelincuentes tengan la oportunidad de explotarlas. Esto no solo mejoraría la seguridad de los sistemas, sino que también contribuiría a la protección de los datos sensibles y la continuidad de los servicios prestados por el INS.

En segundo lugar, la automatización del proceso de detección y corrección de vulnerabilidades reduciría significativamente los tiempos de respuesta ante incidentes de seguridad lo que permitiría a la organización reaccionar de manera más rápida y efectiva frente a las amenazas emergentes. Esta capacidad de respuesta rápida es crucial en un entorno donde los ataques cibernéticos son cada vez más frecuentes y sofisticados. Además, la automatización reduciría la carga de trabajo manual, lo que permitiría al personal de TI del INS centrarse en tareas más estratégicas, como el análisis y la mejora continua de la seguridad.

Por otro lado, el uso de un modelo automatizado basado en las mejores prácticas, herramientas tecnológicas y estándares internacionales de ciberseguridad garantizaría que el INS adopte un enfoque de seguridad alineado con las mejores metodologías del sector. Esto no solo mejoraría la protección de sus sistemas, sino que también facilitaría el cumplimiento de las normativas de seguridad requeridas por las autoridades nacionales e internacionales. De hecho, la adopción de estándares internacionales como el marco NIST (National Institute of Standards and Technology) o las directrices de la ISO/IEC 27001, podría ayudar al INS a fortalecer su postura de seguridad y a reducir los riesgos asociados con las amenazas cibernéticas. (ISO, 2022)

La necesidad de un modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológicas del INS surge de la creciente complejidad de los sistemas informáticos y la proliferación de amenazas cibernéticas. Los ciberataques son cada vez más frecuentes y sofisticados, lo que hace que la detección de vulnerabilidades sea un desafío constante para las organizaciones. Además, la gestión manual de las vulnerabilidades puede ser ineficiente y propensa a errores, lo que aumenta el riesgo de que un atacante explote una vulnerabilidad antes de que sea corregida.

La propuesta a desarrollar mediante la investigación en curso busca reducir estos riesgos al automatizar el proceso de detección y corrección de vulnerabilidades. Al hacerlo, el INS podrá actuar de manera proactiva frente a las amenazas, corrigiendo las vulnerabilidades antes de que sean explotadas. Esto no solo mejorará la seguridad de los sistemas, sino que también contribuirá a la continuidad de los servicios, la protección de los datos sensibles y la confianza de los clientes y socios comerciales del INS.

Antecedentes

La detección y corrección de vulnerabilidades en la infraestructura tecnológica en las instituciones públicas, como el INS, están regidas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), el cual generó en mayo del año 2022 un protocolo para el desarrollo de acciones a implementar ante una amenaza de un ataque de ciberseguridad. Su aplicación, sin embargo, no es supervisada ni controlada al 100 % por esta entidad, entre otras cosas, por falta de recursos, por este motivo en el INS se aplica desde el año 2018, tiempo en el cual se han creado las bases para tener un proceso robusto en este sentido, aunque con muchas oportunidades de mejora, como la automatización de los procesos.

El proceso inició con un total de 1800 vulnerabilidades por atender, estas tenían un retraso de atención de dos años, antes de la instauración del equipo de trabajo para la atención de dichas vulnerabilidades.

Parte de las funciones asignadas a este equipo y proceso son las siguientes:

- Atención de alertas técnicas relacionadas con Ciberseguridad. Fuentes MICITT y SOC GBM.

  Resolución y gestión de IoCs asociados a informes de análisis de vulnerabilidades generados por el departamento de Seguridad de TI del INS.
- Administración proactiva ajustado a metodologías ágiles, asociado al proceso SCRUM y Kanban Dashboard.
- Reforzamiento de la cultura “Ciberseguridad”.

Este proceso se ve apoyado, además, por labores adicionales que se realizan sobre la plataforma tecnológica, como, por ejemplo, la aplicación de parches sobre los servidores Windows, entre otras, que permiten mantener esta parte de la plataforma al día en la seguridad,

sin embargo, esta es una labor que se realiza aun de forma manual, por lo que parte de este proyecto es realizar una propuesta para realizar su automatización con las herramientas que existan en el mercado o a las que el INS actualmente tenga acceso.

En general, se han realizado también diferentes estudios sobre este tema, por ejemplo, algunas tesis que han sido consultadas para reforzar este trabajo y sus conceptos, los siguientes ejemplos tanto del ámbito nacional como internacional ilustran al respecto:

Antecedentes internacionales

1. Propuesta de una implementación de un programa de gestión de vulnerabilidades de seguridad informática para mitigar los siniestros de la información en el policlínico de salud AMC alineado a la NTP-ISO/IEC 27001:2014 en la ciudad de Lima – 2021 (Dávila Angeles & Dextre Alarcón, 2021):

Esta investigación se basó en el establecimiento de un modelo que pudiera gestionar, analizar y evaluar el estado de vulnerabilidades existentes en activos de información en el Policlínico de Salud AMC, esto en Lima Perú, dicho estudio se basó en la norma ISO 27001:2014.

El aporte que brinda este trabajo en la presente investigación está basado en la aplicación de esta norma y su uso en una entidad tan importante como lo es el sector salud, esto recordando que el INS, también cuenta con una subsidiaria que se encuentra en este sector y su implicación es directa con esta área. En este trabajo se hace una descripción muy detallada del funcionamiento del estándar y su aplicación, esto es de ayuda en la presente investigación, pues se pretende en ella establecer y es parte de los objetivos específicos, un modelo que utilice justamente estos estándares y mejores prácticas a nivel internacional. Además, es importante

tener un panorama amplio de la legislación que existe en otros países y como se regulan este tipo de situaciones. También permite ampliar las fronteras en el aspecto del análisis de vulnerabilidades y las diferentes herramientas utilizadas para este tipo de labores.

2. Diseño de una metodología para la detección de ataques a infraestructuras informáticas basada en la correlación de eventos (Pazmiño López, 2017):

En este trabajo se utilizaron diferentes tecnologías que le van a brindar valor a esta investigación, por ejemplo, la OSSTMM e ISAFF, además se diseñó una metodología que permite detectar ataques informáticos a infraestructuras que se basa en la correlación de eventos.

Otro aspecto importante y que aportará valor a esta investigación es la forma en la que se realizaron las simulaciones de los incidentes, pues parte del desarrollo de esta investigación es el montar laboratorios virtuales donde se puedan probar las técnicas y herramientas que se estarán proponiendo como parte de la solución final.

3. Diseño de un sistema de gestión de seguridad de la información para el área de infraestructura tecnológica de Alfragres S.A: basado en la norma ISO / IEC 27001:2013 (Caicedo Carrillo & Rojas Suárez, 2018):

Este trabajo se basa en el diseño de un sistema de Gestión de seguridad de la información en infraestructura para una empresa en específico Alfagres S.A., es una empresa que se dedica a comerciar materiales de construcción al por mayor, artículos de ferretería, etc. Para esta investigación es importante especialmente en la forma en la que se aplica la norma ISO/IEC 27001:2013, pues esta investigación de igual forma pretende basarse en normas técnicas para la implementación de nuestra propuesta de solución.

De igual forma brinda un panorama respecto a la aplicación de las medidas y sistemas de seguridad informáticos para la infraestructura de una empresa de este tipo y que no está en el mismo ámbito del INS, sin embargo, se pueden tomar conclusiones al respecto y mejorar nuestra propuesta.

4. Caso de estudio para el análisis de vulnerabilidad y propuesta de aseguramiento de seguridad de la información en la infraestructura tecnológica de la empresa Nostradamus S.A.S (Mejía Escobar, 2020):

Este trabajo se basa en el estudio y la propuesta de un documento base para la implementación de un sistema de Gestión de Seguridad Informática, basado en la norma ISO 27001, al no ser un proyecto práctico, esto permitirá obtener también información importante para exponer la parte teórica de esta investigación, la forma de aplicar la norma ISO, también se obtendrán datos importantes al respecto de las pruebas prácticas y laboratorios que se realizaron en este proyecto y que pueden ser de utilidad para las pruebas y ejercicios de laboratorios que esta investigación pretende realizar.

5. Modelo de Gestión de riesgo para la infraestructura tecnológica en el GAD Municipal de Flavio Alfaro (Toala Arias & Mazamba Muñoz, 2023):

Este proyecto se basó en el análisis de un modelo de riesgo en una entidad pública de Ecuador, utilizado para identificar, evaluar y gestionar los posibles riesgos que podían afectar los sistemas tecnológicos en dicha organización. Estos riesgos involucraban amenazas a la disponibilidad, confidencialidad, integridad o desempeño de la infraestructura tecnológica.

Con este modelo se logró cuantificar y priorizar esos riesgos basados en su impacto potencial y la probabilidad de que sucedan, para de esta forma tomar decisiones informadas sobre cómo mitigar o eliminar los riesgos.

Este proyecto tiene la particularidad de que fue realizado en una entidad pública al igual que el INS, esto en Ecuador, esto aporta a esta investigación el manejo que se debe realizar en la Gestión de Riesgo de la infraestructura tecnológica en este campo, además aplica varias metodologías que pueden servir como referencia para esta investigación y la forma en la que se estarán obteniendo datos importantes para su realización, tanto a nivel cuantitativo como cualitativo, otro aporte importante a esta investigación extraído de este proyecto es el de cómo realizar una matriz para evaluar riesgos en la infraestructura tecnológica.

Antecedentes nacionales

1. Estrategia para la Gestión de políticas de seguridad informática en una Municipalidad de la Región Chorotega (Villafuerte Guerrero, 2021):

Este trabajo se realizó en una entidad pública, específicamente una Municipalidad en la región de Guanacaste, y su objetivo fue brindar instrumentos de ayuda a esta Municipalidad, en el desarrollo de sus procedimientos y manuales de operaciones, buscando con esto el brindar un servicio eficiente y seguro.

Se utilizaron en este proyecto varios métodos de investigación, por ejemplo, el cuestionario, la observación, entre otras. Finalmente, se presentó un modelo para facilitar la obtención de un adecuado nivel de control de riesgos en el departamento de Tecnologías de Información y Comunicación, permitiendo entre otros evitar y/o disminuir las fallas en los

sistemas, redes, internet y toda la plataforma informática (hardware, software y datos) de ataques o desastres, antes del evento.

El aporte principal que brinda este proyecto de graduación a la presente investigación es principalmente la forma en la que se desarrollaron cuestionarios aplicados a los funcionarios y de esta forma entender su forma de interactuar con TI y con la seguridad informática, esto es esencial, pues los usuarios son uno de los puntos más débiles que pueden existir en la organización y que contrario a los equipos no están sujetos a correcciones y mejoras en la seguridad por lo que conocer al respecto de sus costumbres y educación tecnológica es un elemento muy importante para esta investigación y la solución que se pretende proponer.

2. Evaluación de la Existencia de Políticas de Ciberseguridad en las Pymes y en las Organizaciones del Sector Público que no cuentan con Personal de Ciberseguridad en Costa Rica (Solarte Castañeda, 2021):

Este proyecto tuvo como objetivo evaluar la existencia de políticas de ciberseguridad en las pymes y organizaciones del sector público, cuando estos no cuentan con personal de ciberseguridad en Costa Rica.

Este proyecto de graduación aporta a esta investigación elementos importantes del estudio del comportamiento de las amenazas cibernéticas en el país, esto es importante para contar un panorama amplio y claro del entorno en el que se desenvuelve el INS y la importancia que toma el contar con un esquema robusto en la detección y corrección de vulnerabilidades, además este trabajo está basado en una entidad pública y esto se ajusta a la realidad del INS.

3. Propuesta de un modelo de ciberseguridad para la pequeña empresa en Costa Rica (Leiva Montero, Mantilla Quesada, & Córdoba Retana, 2022):

En este trabajo se utilizaron las normas NIST, con el fin de diseñar la propuesta de un modelo de seguridad informática, en este caso en el sector de las pequeñas empresas en Costa Rica, esto es importante, pues es un enfoque desde un punto de vista de empresas que no cuentan con la posibilidad tecnológica y económica de implementar un modelo de ciberseguridad más robusto, por este motivo, la aplicación de dichas normas ayuda en este sentido a las empresas de este rango.

Este proyecto brinda un aporte importante en la presente investigación, pues se utilizaron herramientas como el NIST, que se pretende utilizar en este trabajo, además de las formas de evaluar los tipos de ciberataques que se han recibido en las pequeñas empresas en Costa Rica, también se brindan estrategias para fomentar la educación tecnológica que se debe tener para asegurar la seguridad cibernética de una empresa.

4. Estrategia nacional de ciberseguridad de Costa Rica 2023-2027 (MICITT, 2023):

Esta estrategia fue emitida desde el año 2017, con el fin de crear una institucionalidad que permita adelantar sus funciones y actividades en cabeza del MICITT y del Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR).

Otro de los objetivos que busca esta estrategia son los de lograr un avance significativo en asuntos de cooperación, de educación y de socialización frente al uso seguro de las Tecnologías de la Información y las Comunicaciones (TIC), de igual forma se deben reforzar los esfuerzos para que se puedan cerrar las brechas en capacidades de ciberseguridad.

La importancia que tiene esta estrategia en el contexto de esta investigación está basada en el hecho de que el INS, al ser una institución pública está supeditada a las directrices emitidas

desde el MICITT, de ahí que este trabajo debe estar ajustado a esta estrategia, por este motivo las pruebas y laboratorios a realizar deben estar en un entorno realista y enfocados en las valoraciones y directrices del Ministerio.

5. Ciberataques y su análisis desde la óptica penal (Quesada Artavia, 2022):

El Ministerio público en este caso apostó por la capacitación de fiscales en la materia de Cibercrimen, a nivel internacional, buscando y tomando en cuenta las tendencias de ese tipo de criminalidad. Se trabaja además en la redacción y en el impulso a nuevas leyes en materia de cibercriminalidad, con el fin de atacar también desde este ángulo estas amenazas.

Este proyecto es importante para esta investigación, porque aporta un enfoque distinto de la ciberseguridad desde la óptica judicial, específicamente en el ámbito penal, esto brinda una visión de las posibilidades y consecuencias que existen en nuestro país, en cuanto a regulación y aspectos legales, esto enriquecerá de gran forma esta parte de la investigación.

Finalmente es importante mencionar que, en la actualidad, se está comenzando a explorar el uso de inteligencia artificial y aprendizaje automático para que estos procesos sean más eficientes. (IBM, 2022)

Proyecciones

Alcances

El presente trabajo tiene como propósito principal el diseño de un modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS). Este modelo busca optimizar los procesos de seguridad informática del INS, minimizando el riesgo de ciberataques y mejorando la resiliencia de los sistemas tecnológicos de la Institución. Para ello, se abordarán los siguientes alcances:

En primera instancia, se realizará un diagnóstico exhaustivo de los procesos actuales utilizados por el departamento de Operación y Soporte Técnico del INS para identificar y corregir vulnerabilidades. Este análisis permitirá identificar las brechas existentes y las oportunidades de mejora, con el objetivo de optimizar la eficiencia de la detección y corrección de vulnerabilidades.

Se llevará a cabo una consulta detallada de estándares internacionales de ciberseguridad y mejores prácticas, con el fin de establecer los requerimientos y especificaciones técnicas necesarias para desarrollar un modelo automatizado de detección y corrección de vulnerabilidades. Esto incluirá la identificación de herramientas tecnológicas avanzadas, metodologías ágiles y marcos de trabajo como el NIST (National Institue of Standards and Technology), ISO/IEC 27001, entre otros, que sean relevantes para el diseño del modelo.

Existen además otros riesgos de ciberseguridad en el sector de seguros, se debe recordar que los ataques cibernéticos son intentos exitosos o no, por acceder a información, o sistemas de información sin autorización con el fin de robar o alterar la información o bloquear sistemas de información. (IAIS, 2019)

El sector financiero es particularmente vulnerable a los ataques cibernéticos porque, entre otros motivos, las empresas tienen en su poder valiosos datos personales de los consumidores y activos financieros.

De acuerdo con el Documento de Aplicación de la IAIS sobre la Supervisión de la Ciberseguridad del Asegurador del año 2018 (IAIS, 2019), se deben aplicar los G7FE que son un conjunto conciso de principios de ciberseguridad no vinculantes para entidades públicas y privadas que operan en el sector financiero, cuyo objetivo es ser útil tanto a las empresas como a los supervisores, existen ocho elementos fundamentales que se indican a continuación:

- Estrategia y marco de ciberseguridad
- Gobernanza
- Evaluación y control de riesgo
- Monitoreo
- Respuesta
- Recuperación
- Intercambio de información
- Aprendizaje continuo

El diseño del modelo automatizado incluirá la creación de un sistema que utilice tecnologías avanzadas para la identificación y corrección de vulnerabilidades de manera proactiva, con el objetivo de optimizar la seguridad y reducir la intervención manual en los procesos. Este modelo estará basado en metodologías ágiles que permitan una integración fluida y eficiente dentro de la infraestructura tecnológica del INS.

El modelo propuesto incluirá la integración de herramientas tecnológicas avanzadas, como sistemas de monitoreo continuo y software de análisis de vulnerabilidades, que permitan detectar y corregir problemas de manera automatizada. Además, se fomentará el uso de metodologías ágiles para facilitar la implementación rápida y la adaptación continua a nuevas amenazas y vulnerabilidades.

Se propondrá un marco para evaluar la efectividad del modelo, incluyendo métricas de desempeño como la rapidez y la detección y corrección de vulnerabilidades, la reducción de riesgos asociados a ciberataques y la eficiencia operativa de los procesos automatizados.

Limitaciones

A pesar de que el proyecto tiene como objetivo el desarrollo de un modelo automatizado que optimice la detección y corrección de vulnerabilidades, existen varias limitaciones que deben ser consideradas en el alcance de la investigación.

La efectividad del modelo propuesto dependerá en gran medida de la infraestructura tecnológica del INS. Cualquier limitación en los recursos actuales, como la capacidad de los servidores, la compatibilidad de los sistemas con las herramientas propuestas, o la falta de un entorno adecuado para la implementación de soluciones automatizadas, puede restringir la eficacia del modelo.

Dado que este trabajo está destinado a ser realizado dentro de un período específico, el modelo automatizado no se implementará completamente en la infraestructura del INS. En su lugar, se proporcionará una propuesta detallada y un prototipo de modelo, pero la implementación real dependerá de los recursos y el tiempo disponibles después de la conclusión del proyecto.

La implementación de un modelo automatizado en una organización puede enfrentar resistencia debido a la falta de familiaridad con las nuevas tecnologías o al temor de que la automatización pueda reemplazar funciones humanas. Es posible que la integración de nuevas herramientas y metodologías ágiles requiera un proceso de capacitación del personal y adaptación cultural dentro del INS, lo que puede afectar la rapidez con que se adopten las nuevas soluciones.

A pesar de la automatización de los procesos de detección y corrección, algunos tipos de vulnerabilidades, como aquellas que afectan a componentes específicos del sistema o son explotadas de forma inédita por ciberdelincuentes, podrían no ser detectadas o corregidas de

manera automática. La evolución constante de las amenazas cibernéticas puede dificultar la cobertura total de las vulnerabilidades a través de un modelo único.

El trabajo está sujeto a la disponibilidad y accesibilidad de las herramientas tecnológicas necesarias para la implementación del modelo, así como la colaboración de los equipos internos del INS. Cualquier restricción en el acceso a estas herramientas o la falta de soporte de estas podría limitar el alcance de la propuesta.

El modelo automatizado se centrará exclusivamente en la infraestructura tecnológica y la seguridad informática, por lo que otros aspectos de seguridad, como la protección física de los activos o la capacitación en seguridad para los empleados, no serán tratados dentro de este proyecto.

CAPÍTULO 2: MARCO TEÓRICO

El presente capítulo tiene como objetivo dar a conocer los fundamentos teóricos y conceptuales necesarios para la correcta comprensión y justificación del proyecto, este capítulo abordará los principales conceptos, teorías, modelos y prácticas que sustentan el diseño de un modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS), se cubrirán desde la historia y estructura organizacional del INS hasta los marcos de ciberseguridad, las metodologías ágiles, y las tecnologías de automatización en el campo de la seguridad informática.

1. Historia del Instituto Nacional de Seguros (INS)

En esta sección se presentará un repaso histórico de la fundación y evolución del INS, destacando su papel en la economía nacional y su impacto en el sector asegurador en Costa Rica. Además, se incluirá información relevante sobre su transformación digital y los esfuerzos para modernizar sus sistemas de infraestructura tecnológica para brindar mejores servicios a los ciudadanos.

Fundación del INS

El Instituto Nacional de Seguros (INS) se fundó mediante la Ley 12, el 30 de octubre de 1924. En sus inicios se llamó Banco Nacional de Seguros, pero cambió su nombre en mayo de 1948 a Instituto Nacional de Seguros por medio de un decreto. Mantuvo a su cargo la administración del monopolio de seguros desde su creación hasta el 7 de agosto de 2008 cuando entró en vigor la Ley 8653 “Ley Reguladora del Mercado de Seguros”, que abrió el mercado y trajo la competencia. (INS, 2024)

Desarrollo y Expansión

El Instituto Nacional de Seguros es una empresa aseguradora líder en el mercado nacional y de las más importantes de Centroamérica y el Caribe, por este motivo, el contar con una infraestructura tecnológica adecuada y que brinde la seguridad que los clientes y socios comerciales requieren es fundamental para el éxito de la empresa. (INS, 2024)

Adopción de nuevas tecnologías

En este mercado competitivo la adopción de nuevas tecnologías enfocadas en la atención del cliente y en mejorar su experiencia dentro de cada una de las oficinas del grupo INS, es un punto básico en el desarrollo de la empresa. Por este motivo, se ha creado la Dirección de Transformación digital que en conjunto con otras dependencias se encarga de investigar y buscar nuevas opciones tecnológicas que faciliten al usuario sus trámites, se sientan más cómodos y seguros al utilizar cualquiera de las herramientas a su alcance.

Dentro de esta transformación digital, la Dirección de Tecnologías de información es parte clave, pues desde esta dependencia se gestionan e implementan la mayoría de estos cambios tanto en infraestructura como en software.

2. Misión y Visión del INS

El INS tiene definidas dentro del marco institucional la siguiente misión y visión:

- Misión: Somos el INS, la aseguradora que brinda protección y prevención con función social, que genera valor sostenible (INS, 2024)
- Visión: Ser la mejor experiencia aseguradora (INS, 2024)

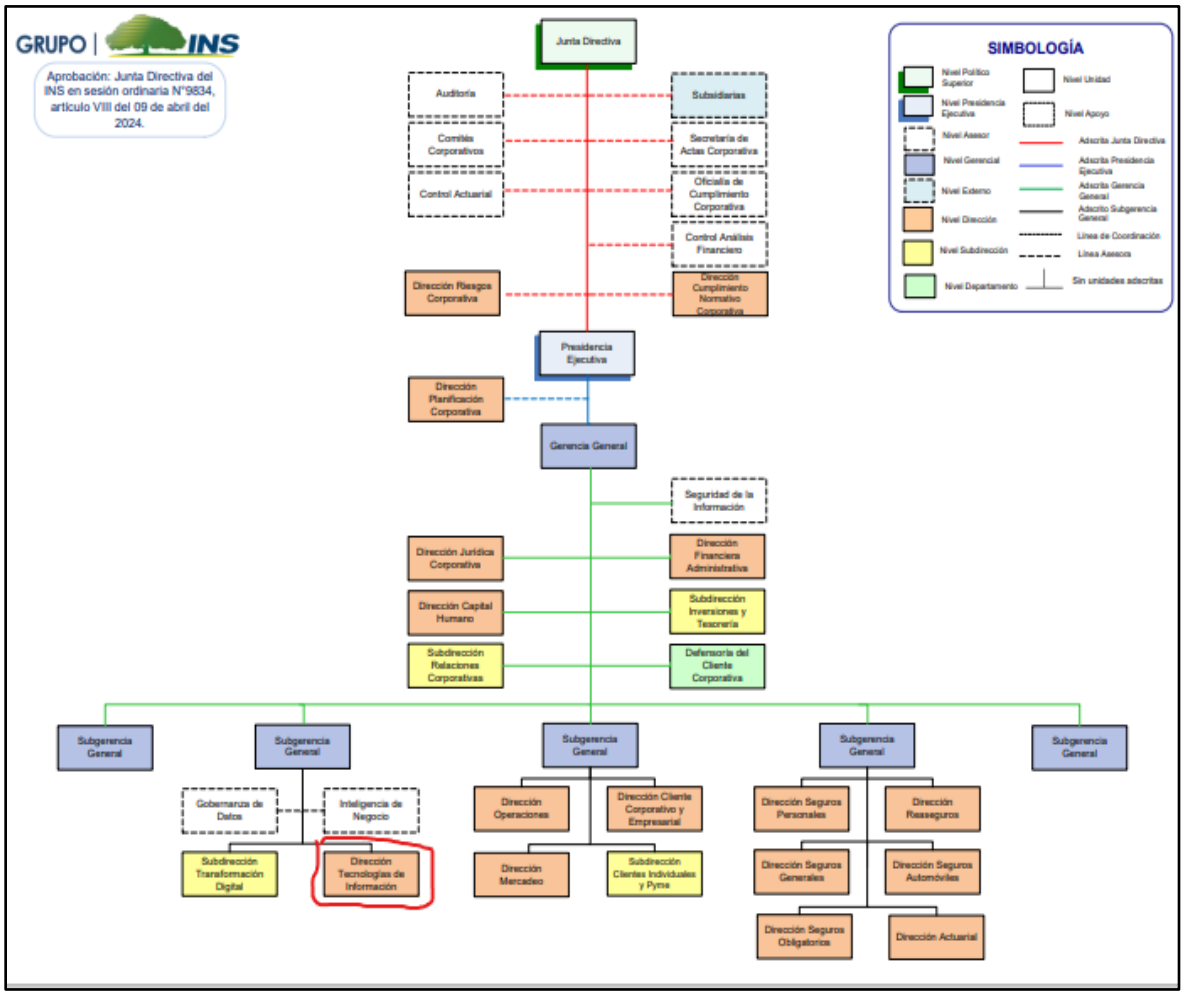
3. Estructura organizacional del INS

En este apartado se describirá la estructura organizacional del INS, con un énfasis particular en el departamento responsable de la seguridad tecnológica, como lo es el departamento de Operaciones y Soporte Técnico.

Organigrama del INS

Figura 1

Organigrama del INS



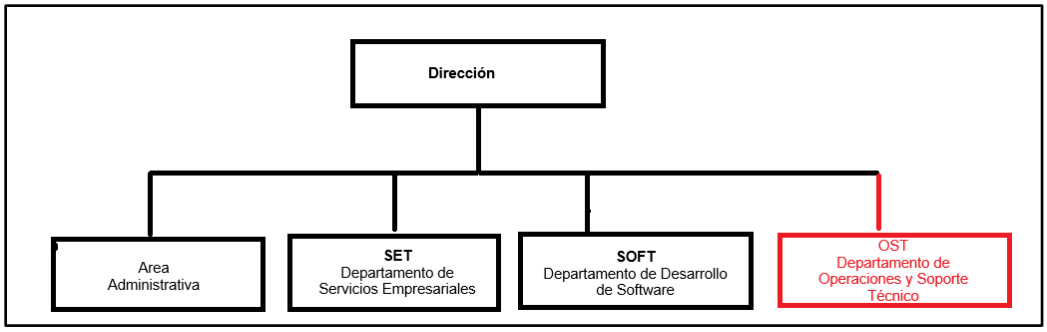
Nota. Fuente: (INS, 2024)

Organigrama de la Dirección de Tecnologías de Información

En la siguiente figura se muestra el organigrama actual de la Dirección de Tecnologías de Información del Instituto Nacional de Seguros.

Figura 2

Organigrama de TI

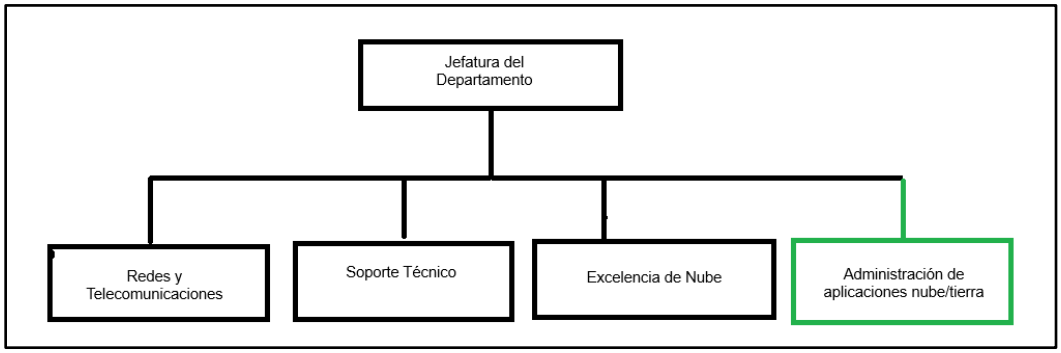


Organigrama del Departamento de Operaciones y Soporte Técnico

En la siguiente figura se muestra el organigrama actual del departamento de Operaciones y Soporte Técnico.

Figura 3

Organigrama de OST



Roles y responsabilidades

Dentro del aspecto de ciberseguridad, existe en la estructura del INS una estructura claramente definida, y que deriva en el grupo especializado para la atención y corrección de

vulnerabilidades dentro de la infraestructura tecnológica, dicha estructura se describe a continuación (INS D. d., 2022):

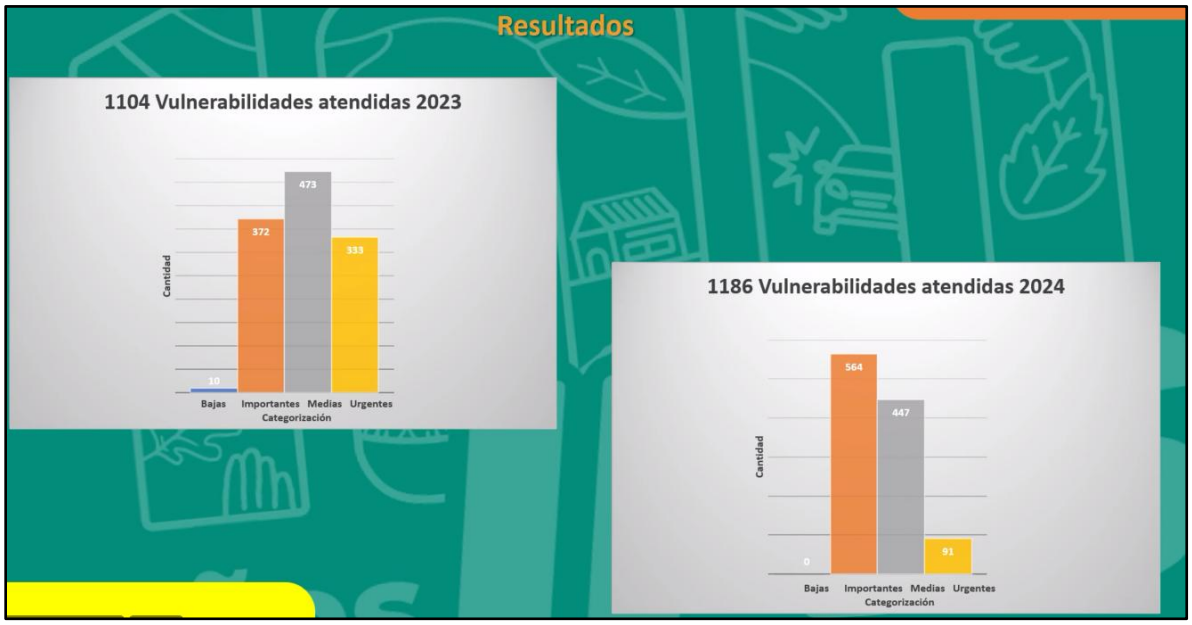
- Dirección de Tecnologías de Información: la Dirección a la cabeza de la Jefatura respectiva es la primera responsable de gestionar los recursos necesarios para la atención de los temas de seguridad informática, además de realizar las siguientes funciones: resolución de impedimentos a nivel ejecutivo, ser facilitadores de las funciones y tiempos, presentar resultados ante la administración superior.
- Seguridad TIC: es un departamento adscrito a la Dirección, compuesto por funcionarios especialistas en temas de ciberseguridad, que tiene entre sus principales funciones las siguientes: ejecución de análisis de vulnerabilidades, re-testing, seguimiento y fiscalización de mitigación, elaboración y gestión de documentación, carga de tablero con resultados y pendientes.
- Departamento de Operación y Soporte Técnico: este departamento a través de su jefatura se encarga de gestionar y coordinar la célula para atención de vulnerabilidades llamada Chirripó, entre sus funciones además se encuentran las de ser un facilitador y precursor de recursos antes las diferentes dependencias y la Dirección de TI.
- Célula de atención de vulnerabilidades Chirripó: este es un grupo multidepartamental compuesto por funcionarios de varias dependencias y especialidades que se encargan de dar atención a las vulnerabilidades obtenidas en los escaneos que realizan desde el departamento de Seguridad de TIC, entre sus principales funciones se encuentran las siguientes: atención de alertas técnicas relacionadas con Ciberseguridad que provienen de fuentes como el MICITT y

SOC GBM, resolución y gestión de IoCs asociados a informes de análisis de vulnerabilidades generadas por Seguridad de TIC, administración proactiva ajustada a metodologías ágiles, asociadas al proceso SCRUM y Kanban Dashboard, reforzar la cultura ciberseguridad en la población institucional.

En la siguiente imagen se pueden observar algunos de los resultados obtenidos por este grupo en los años 2023, 2024:

Figura 4

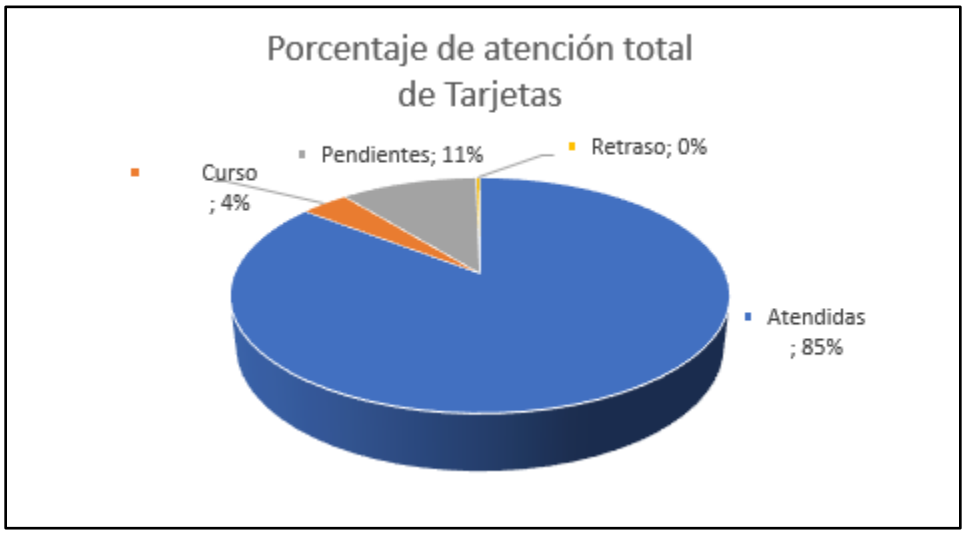
Resultados grupo Chirripó



Nota. Fuente: (INS D. d., 2022)

Figura 5

Porcentaje de atención de tarjetas grupo Chirripó



Nota. Fuente: (INS D. d., 2022)

4. Infraestructura tecnológica y de ciberseguridad del INS

En esta sección se hará una descripción de los elementos propios de la infraestructura tecnológica del INS, relacionados específicamente con la seguridad informática y operaciones críticas.

Infraestructura tecnológica

El INS cuenta con una amplia infraestructura tecnológica, con una clara tendencia en los últimos años a la migración de elementos a la nube, por lo tanto, es posible hablar de un ecosistema híbrido, un amplio porcentaje de esta infraestructura sobre todo en lo que a servidores se refiere (95 %), se encuentra virtualizado en la plataforma VMWare tanto en su modalidad On Premise, como en su modalidad AVS (Azure VMware Solution), en la siguiente tabla se especifican los números respectivos:

Tabla 1

Distribución de servidores por plataforma

Plataforma	Número de Servidores
VMWare- On Premise	215
AVS (Azure VMWare Solution)	665
Servidores físicos en nube GBM	4
Servidores físicos en Centro de Datos del INS	4
TOTAL	888

Nota. Fuente: Elaboración propia

En lo que respecta a sistemas operativos utilizados en la infraestructura tecnológica se encuentran los siguientes:

- Microsoft Windows Server (2016.2019.2022)
- Linux (Red Hat Linux 9.4)
- AIX
- OS400

Ciberseguridad en el INS

Se describirán las políticas, medidas, y tecnologías implementadas para proteger la infraestructura contra ciberataques. (INS D. d., 2022)

- Contrato con el SOC de GBM
- Políticas de cambio de clave de acceso mensual
- Políticas de Múltiple factor de autenticación para acceso a aplicaciones
- Políticas de bloqueo de uso de dispositivos USB para almacenamiento de información

- Controles de acceso a los diferentes sistemas
- Aplicación de firewall y sistemas de protección perimetral
- Sistema de monitoreo de la red y detección de intrusos
- Conformación de grupo Chirripó para atención de vulnerabilidades
- Sistemas de backup (Avamar)
- Sistemas de replicación de servidores de VMWare para la recuperación ante desastres (Recovery Manager)

5. Vulnerabilidades en la infraestructura tecnológica

En este punto se generarán varias definiciones tendientes a brindar un panorama más claro de lo que significan las vulnerabilidades y los daños que la explotación de estas pueden causar en la infraestructura tecnológica de una organización. Además, se explicará en qué consiste la gestión de vulnerabilidades y los diferentes métodos existentes para la identificación y corrección de vulnerabilidades.

Qué es vulnerabilidad

De acuerdo con el Instituto Nacional de Ciberseguridad de España una vulnerabilidad es un fallo técnico o deficiencia de un programa que puede permitir un usuario no legitimado acceda a la información o lleva a cabo operaciones no permitidas de manera remota. (INCIBE, 2024)

Existen varios tipos de vulnerabilidades identificadas, a continuación, se detallan algunas de las más conocidas (CampusCiberseguridad, 2023):

- Errores en la gestión de recursos: una aplicación permite que se consuman en exceso de recursos afectando a la disponibilidad de estos.

- Error de configuración: problemas de configuración de software o de los servicios web.
- Factor humano: negligencias causadas generalmente por la falta de formación y concienciación.
- Validación de entrada: fallo en la validación de datos introducidos en aplicaciones.
- Salto de directorio: fallo en la depuración de un programa, en la validación de caracteres especiales.
- Permisos, privilegios y/o control de acceso: fallos en la protección y gestión de permisos.

Causas comunes de vulnerabilidades

Existen varias causas que se pueden denominar como las más comunes en cuanto a las vulnerabilidades, de acuerdo con IBM y al instituto Ponemon, las filtraciones de datos han alcanzado cifras récord en los últimos años, con un promedio de casi 2200 ataques cibernéticos diarios, que acarrean costos aproximados de 4,24 millones de dólares por ataques a empresas grandes. (EASYDMARC, 2023)

A continuación, se nombran algunas de las causas más comunes que se presentan aun en nuestros días:

- Contraseñas débiles
- Piratería criminal
- Vulnerabilidades de aplicaciones y puertas traseras
- Ingeniería social
- Suplantación de identidad, malware y ransomware

- Gestión inadecuada de permisos
- Errores de usuarios y amenazas internas
- Amenazas físicas

Clasificación de vulnerabilidades:

Las vulnerabilidades se pueden clasificar de acuerdo con su origen en los siguientes tipos:

- Vulnerabilidades en servidores (Sistemas operativos, puertos, protocolos)
- Vulnerabilidades en aplicaciones (código, falta de controles adecuados)
- Vulnerabilidades en elementos periféricos (redes)
- Vulnerabilidades humanas (mala gestión de contraseñas, cultura en ciberseguridad)

Impacto de las vulnerabilidades en la seguridad

El impacto de la materialización de una vulnerabilidad en una organización independientemente del tipo que esta sea, y más aun tratándose de una empresa como el INS, cuyo fin es brindar seguridad a sus clientes en todo aspecto, va desde la parte económica, como desde la parte reputacional, pues esto puede traducirse no solo en robo de información, sino en pérdida de servicios claves por largo tiempo.

Para ejemplificar aún más lo que este tipo de amenazas puede causar en una organización se mencionan los ataques e incidentes de seguridad más relevantes que impactaron a las organizaciones en América Latina en 2024, esto de acuerdo con la página de información Delfino.cr y basado en un estudio del Laboratorio de Investigación de ESET Latinoamérica (eset, 2024)

- Banco do Brasil: un ataque enfocado en los empleados de la institución y que permitió a los atacantes acceder a las bases de datos del banco, con saldo de robo

de datos personales y financieros por más de 2 millones de clientes lo que representó un total de 40 millones de reales en delitos financieros.

- Interbank: filtración de datos en este banco que es uno de los más fuertes de Perú, el atacante accedió a datos sensibles de clientes de la entidad, utilizando credenciales internas para acceder a servidores, el saldo fue la exposición de datos de más de 3 millones de usuarios y la exigencia de $4 millones exigidos al banco.
- Coppel: cadena mexicana de tiendas que afectó a 1800 sucursales en todo este país, dicho ataque afectó las operaciones por 3 meses, esto significó para la empresa una pérdida cercana a los $15 millones en ingresos, el origen de este ataque fue un ransomware conocido como Lockbit 3.0.
- Grupo Bimbo: esta empresa sufrió un ataque de ransomware en febrero del 2024, provocado por el grupo Medusa, esto provoco que dicho grupo solicitara a esta empresa un rescate de $6.5 millones.

6. Incidentes de ciberseguridad

En el contexto de la ciberseguridad, es crucial conocer los diferentes tipos de ciberataques que pueden afectar a una organización, como el Instituto Nacional de Seguros (INS). Los ciberataques son ataques maliciosos que buscan dañar, robar o manipular sistemas informáticos, redes o datos con fines fraudulentos o destructivos. Este apartado tiene como objetivo proporcionar una visión general de los principales tipos de ciberataques que podrían amenazar la infraestructura tecnológica del INS.

Malware (software malicioso)

De acuerdo con la página redhat.com, el malware se define como un software malicioso e incluye cualquier sistema de software que afecte los intereses del usuario, puede afectar no solo a

la computadora o al dispositivo infectados, sino también a cualquier otro dispositivo con el que este pueda comunicarse. (Redhat, 2018)

Existen varios tipos de malware, estos son los más conocidos:

- Troyanos: son archivos ejecutables que se propagan a través de la ingeniería social, se hacen pasar por otro software para persuadir a los usuarios incautos de que los abran y en consecuencia inicien el archivo ejecutable. (Redhat, 2018)
- Gusanos: los gusanos se introducen en lugares no deseados, los primeros conocidos datan de 1980, con la aparición y auge del internet los piratas informáticos y los desarrolladores de malware han diseñado gusanos que se copian a sí mismos a través de las redes, lo cual los convirtió en una pronta amenaza para las empresas y los usuarios conectados a la Web. (Redhat, 2018)
- Exploits: es un punto vulnerable del software que podría utilizarse ilegalmente para forzarlo a realizar alguna tarea fuera de su función original. Un programa de malware puede usarlo para ingresar a un sistema o para trasladarse de una parte del sistema a otra. (Redhat, 2018)
- Ransomware: es una forma de malware que exige un pago a cambio de su anulación, muchos cifran archivos en el sistema de un usuario y exigen el pago de un rescate en Bitcoin a cambio de una clave de descifrado, adquirió notoriedad a mediados de la década de 2000, desde ese momento sigue siendo un de las amenazas de seguridad informática más graves y generalizadas. (Redhat, 2018)

Phishing

De acuerdo con IBM, el phishing es un tipo de ciberataque que utiliza emails, mensajes de texto, llamadas telefónicas o sitios web fraudulentos con el fin de engañar a los usuarios para obtener datos sensitivos, descargar malware, o exponer datos sensitivos a cibercriminales.

Este tipo de ataques son una forma de ingeniería social, a diferencia de otros tipos de ciberataques que atacan directamente redes y recursos informáticos, los ataques de ingeniería social utilizan el error humano. (IBM, 2024)

Algunos tipos de phishing son:

- Spear phishing: es un ataque de phishing dirigido contra un individuo específico, el objetivo suele ser alguien con acceso privilegiado a datos sensibles o autoridad especial que el atacante pueda explotar, como un gestor financiero que pueda mover dinero de cuentas de la empresa.
- Smishing: SMS phishing es un tipo de ataque que utiliza mensajes de texto falsos para engañar objetivos, los estafadores suelen hacerse pasar por el proveedor inalámbrico de la víctima, enviando un texto que ofrece un regalo gratuito o le pide al usuario que actualice la información de su tarjeta de crédito.

  Vishing: el phishing de voz, o vishing, es phishing por llamada telefónica, los incidentes de este tipo han aumentado en los últimos años en un 260 %, esto en parte se debe a la disponibilidad de voz sobre la tecnología IP (VoIP), que los estafadores pueden utilizar para hacer millones de llamadas vishing automatizadas por día. (IBM, 2023)

Ataques de denegación de servicio (DoS) y denegación de servicio distribuida (DDoS)

De acuerdo con el Instituto Nacional de Ciberseguridad de España, este tipo de ataques tienen como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser la aplicación o el canal de transmisión, como a la red informática.

Este tipo de ataques tiene dos técnicas: la denegación de servicio (DoS) y la denegación de servicio distribuido (DDoS), la diferencia entre ambos es la cantidad de servidores o computadoras que realizan el ataque.

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o IP, consumiendo así los recursos que ofrece este servicio, hasta llegar a agotar la capacidad de respuesta y empieza a denegar peticiones.

En los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de máquinas o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque, este tipo de ataque es más difícil de detectar, pues el número de peticiones proviene desde diferentes IPSy el administrador no puede bloquear la IP que está realizando las peticiones, como si ocurre en los ataques DoS. (INCIBE, 2024)

¿Cómo evitar un ataque de este tipo?

Existen varias formas de evitar este tipo de ataques, por ejemplo: revisar la configuración de los routers y firewalls con el fin de detectar IP’s no válidas o falsas, que provengan de posibles atacantes. (INCIBE, 2024)

Otros métodos de prevención de ataques DoS son:

- Reducción de superficie de ataque

- Difusión de red Anycast
- Monitoreo de amenazas adaptable y en tiempo real
- Almacenamiento en caché
- Limitación de velocidad

Algunas herramientas para mitigación de ataques DDoS son:

- Firewall de aplicaciones web (WAF)
- Mitigación de DDoS siempre activa

Ataques de inyección

Un ataque de inyección es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos. Una vez dentro, puede controlar la base de datos del sitio web y secuestrar la información de los usuarios. (AVAST, 2022)

- SQL Injection: se producen cuando un hacker introduce o inyecta en el sitio web código SQL malicioso, un tipo de malware que se conoce como la carga útil, y consigue subrepticiamente que envíe ese código a su base de datos como si de una consulta legítima se tratara. Estos ataques únicamente son viables cuando un sitio web carece de un saneamiento de entrada adecuado: el proceso que vela por que la información que introducen los usuarios finales no pueda colarse por ningún resquicio y funcionar como código ejecutable en el servidor. (AVAST, 2022)
- Cross-Site Scripting (XSS): este tipo de ataques entre sitios consisten en inyectar códigos maliciosos en sitios web que suelen ser fiables. Un ataque de scripting entre sitios se produce cuando los ciberdelincuentes inyectan scripts maliciosos en el contenido del sitio web atacado, que luego se agrega al contenido dinámico que

se envía al navegador de la víctima, este desconoce que los scripts maliciosos no son fiables y, por lo tanto, los ejecuta. Al hacer esto los scripts pueden acceder a las cookies, los tokens de sesión u otra información confidencial retenida por el navegador. (Karspersky, 2024)

- Command Injection: la inyección de comandos es un ataque cuyo objetivo es la ejecución de comandos arbitrarios en el sistema operativo host a través de una aplicación vulnerable. Son posibles cuando una aplicación pasa datos no seguros proporcionados por el usuario (formularios, cookies, encabezados HTTP,etc) a un shell del sistema. En este ataque, los comandos del sistema operativo proporcionados por el atacante se ejecutan generalmente con los privilegios de la aplicación vulnerable. Los ataques de inyección de comandos son posibles en gran medida debido a una validación de entrada insuficiente. En la inyección de comandos, el atacante extiende la funcionalidad predeterminada de la aplicación, que ejecuta comandos del sistema sin necesidad de inyectar código. (OWASP, 2024)

Ataques de hombre en el medio (MITM)

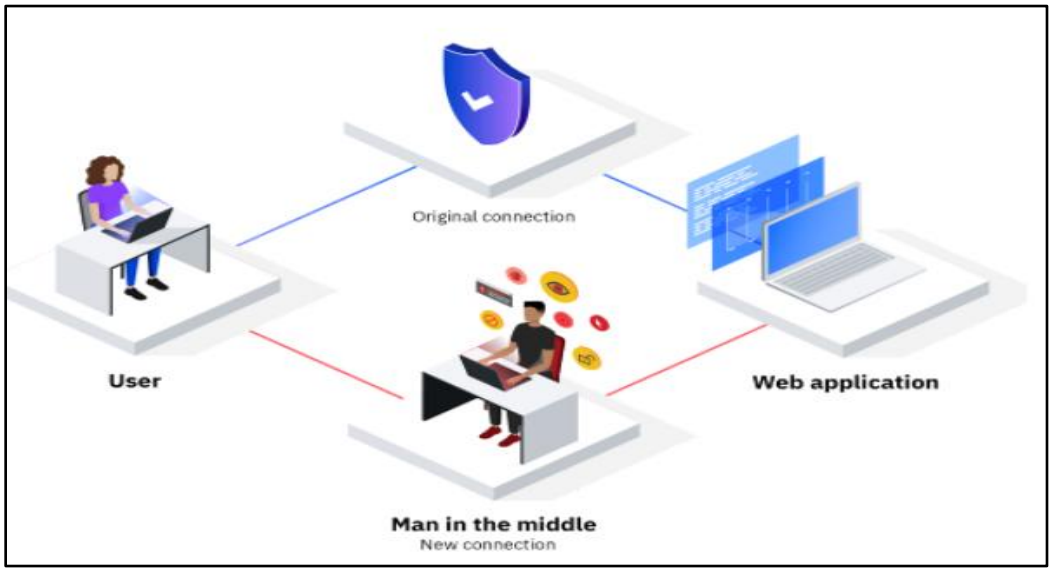
Este es un tipo de ataque cibernético en el que un hacker roba información confidencial al espiar las comunicaciones entre dos objetivos en línea, como un usuario y una aplicación sitio web.

Luego de colocar sigilosamente en medio de comunicaciones bipartitas, los atacantes MITM interceptan datos confidenciales, como números de tarjetas de crédito, información de cuentas y credenciales de inicio de sesión, luego emplean esa información para cometer otros

delitos cibernéticos, como realizar compras no autorizadas, secuestrar cuentas financieras y robar identidad. (IBM, 2024)

Figura 6

Ataque MITM(Man in the middle)



Nota. Fuente (IBM, 2023)

Para ejemplificar los alcances de este tipo de ataques, están los siguientes ejemplos:

- Equifax: en el 2017 esta empresa de reportes crediticios fue víctima de un ataque de intermediario debido a una vulnerabilidad sin parches en el marco de su aplicación sitio web. El ataque expuso la información financiera de casi 150 millones de personas.
- DigiNotar: en el año 2011 hackers lanzaron un ataque de MITM exitoso contra la autoridad de seguridad digital holandesa DigiNotar, esto lo lograron utilizando sitios web falsos para recopilar contraseñas. Esta filtración hizo que la empresa emitiera más de 500 certificados de seguridad comprometidos a los principales

sitios web como Google o Yahoo, finalmente la empresa fue eliminada como proveedora de certificados de seguridad y se declaró en quiebra.

- Tesla: en el 2024 los investigadores informan que una vulnerabilidad permite a los hackers lanzar un ataque MITM para desbloquear y robar vehículos Tesla. (IBM, 2023)

¿Cómo prevenir este tipo de ataques?

Entre las estrategias más recomendadas por los expertos para mitigar y prevenir este tipo de amenazas se indican las siguientes:

- Sitios web seguros (HTTPS): los usuarios únicamente deben visitar sitios web seguros, esto es indicado por el https y un icono de candado en la barra de direcciones del navegador, además los protocolos SSL y TLS (Transport Layer Security) para aplicaciones pueden proteger contra el tráfico sitio web malicioso y prevenir ataques de suplantación de identidad.
- Seguridad de los endpoints: los endpoints como computadoras portátiles, smartphones, estaciones de trabajo y servidores, son objetivos principales de los atacantes MITM. La seguridad de estos dispositivos, incluidos los últimos parches y software antivirus, es fundamental para evitar que los atacantes instalen malware en ellos.
- Redes privadas virtuales (VPN): una VPN proporciona una fuerte defensa contra los ataques MITM al cifrar el tráfico de la red. Incluso si se produce una violación, los piratas informáticos no podrán leer datos confidenciales como credenciales de inicio de sesión, números de tarjetas de créditos e información de cuenta.

- Autenticación multifactor (MFA): MFA requiere un paso adicional más allá de introducir una contraseña para acceder a cuentas, dispositivos o servicios de red. Incluso si un atacante MITM puede obtener credenciales de inicio de sesión.
- Cifrado: el cifrado es fundamental en la seguridad de una red y la defensa contra los ataques MITM. Un cifrado estable de extremo a extremo en todo el tráfico y los recursos de la red, incluido el contenido del email, los registros DNS, las aplicaciones de mensajería y los puntos de acceso, puede frustrar muchos ataques MITM.
- Redes wifi públicas: los usuarios deben evitar redes wifi públicas al realizar transacciones que involucran datos confidenciales, como el realizar compras o transacciones bancarias. (IBM, 2023)

Exploits y vulnerabilidades de día cero

Este tipo de ataque es una técnica de ciberataque que aprovecha un fallo de seguridad desconocido o no corregido en el software, hardware o firmware de un servidor. El término "día cero" hace referencia al hecho de que el proveedor de software o dispositivos dispone de un total de cero días, es decir, que no dispone de tiempo alguno para corregir el fallo, pues los agentes maliciosos pueden utilizarlo para acceder a los sistemas vulnerables.

Un ataque de día cero se produce cuando un actor malintencionado utiliza un exploit de día cero para introducir malware, robar datos o causar daños a usuarios, organizaciones o sistemas.

Según IBM, el equipo denominado X-Force Threat Intelligence ha registrado 7327 vulnerabilidades de día cero desde 1988, si bien es cierto, esto supone únicamente el 3 % de todas las vulnerabilidades de seguridad registradas, la vulnerabilidades de día cero se encuentran entre los riesgos de seguridad más graves, porque dejan a un gran número de usuarios u organizaciones enteras totalmente expuestos a la ciberdelincuencia hasta que el proveedor o la comunidad de ciberseguridad identifican el problema y publican una solución. (IBM, 2023)

El ciclo de vida de una vulnerabilidad de día cero existe en una versión de sistema operativo, aplicación o dispositivo desde que es lanzado, situación que es ignorada por el usuario, esta circunstancia puede pasar desapercibida por días, meses o años hasta ser detectada.

Normalmente los hackers suelen desarrollar exploits más rápido de lo que los equipos de seguridad desarrollan parches, según estimaciones, los exploits suelen estar disponibles en los 14 días siguientes a la divulgación de una vulnerabilidad. Sin embargo, una vez iniciados los ataques, los parches suelen estar listos pocos días después.

Algunos de ejemplos de ataques de este tipo que han sido realizados son los siguientes:

- Stuxnet: era un sofisticado gusano informático que sacaba provecho de cuatro vulnerabilidades de software de día cero diferentes en los sistemas operativos de Microsoft Windows.
- Log4Shell: era una vulnerabilidad de día cero en Log4J, una biblioteca Java de código abierto utilizada para registrar mensajes de error, los hackers podrían usar este fallo para controlar a distancia casi cualquier dispositivo que ejecute aplicaciones Java.

- Ataques a Chrome en 2022: hackers norcoreanos explotaron una vulnerabilidad de ejecución remota de código de día cero en los navegadores web Google Chrome, mediante técnicas de phishing remitían a las víctimas a sitios falsos que aprovechaban la vulnerabilidad de Chrome e instalaban spyware y malware de acceso remoto en los equipos de las víctimas.

Existen algunas opciones para prevenir y evitar este tipo de vulnerabilidades, las más importantes son las siguientes:

Gestión de parches: un programa formal de gestión de parches puede ayudar a los equipos de seguridad a estar al tanto de los parches críticos que sean generados por los proveedores.

- Gestión de vulnerabilidades: la evaluación en profundidad de las vulnerabilidades y las pruebas de penetración pueden ayudar a las empresas a encontrar vulnerabilidades de día cero en sus sistemas antes de que lo hagan los hackers.
- Gestión de la superficie de ataque (ASM): las herramientas ASM permiten a los equipos de seguridad identificar todos los activos de sus redes y examinarlos en busca de vulnerabilidades.
- Información sobre amenazas: los investigadores de seguridad suelen ser de los primeros en detectar vulnerabilidades de día cero. Las organizaciones que se mantienen al día con la inteligencia de amenazas externas suelen enterarse antes de las nuevas vulnerabilidades de día cero.
- Métodos de detección basados en anomalías: el malware de día cero puede eludir los métodos de detección basados en firmas, pero las herramientas que utilizan el

machine learning para localizar actividades sospechosas en tiempo real suelen ser capaces de detectar ataques de día cero.

- Arquitectura zero trust: la arquitectura de confianza cero puede limitar los daños cuando existe alguna vulnerabilidad en la infraestructura, esta técnica utiliza la autenticación continua y el acceso con mínimos privilegios para impedir los movimientos laterales y bloquear el acceso de los agentes malintencionados a los recursos sensibles. (IBM, 2023)

Ataques de contraseña y fuerza bruta

Un ataque de fuerza bruta es el que utiliza el método de ensayo y error para adivinar la información de inicio de sesión, las claves de cifrado o encontrar una página web oculta. Estos ataques se realizan por fuerza bruta, lo que significa que utilizan intentos de fuerza excesivos para intentar forzar su entrada en las cuentas privadas.

Este método de ataque es antiguo, pero sigue siendo eficaz y goza de popularidad entre los hackers, en función de la longitud y complejidad de la contraseña, descifrarla puede llevar desde unos segundos hasta varios años.

Algunas de las ventajas que los hackers obtienen de este tipo de ataques son las siguientes:

- Sacar provecho de los anuncios o recopilar datos de actividad
- Robo de datos personales y objetos de valor
- Difusión de malware para causar perturbaciones
- Secuestro de tu sistema para actividades maliciosas
- Arruinar la reputación de un sitio web

Existen varios tipos de ataques de fuerza bruta, algunos de ellos son los siguientes:

- Ataques simples de fuerza bruta
- Ataques de diccionario
- Ataques híbridos de fuerza bruta
- Ataques de fuerza bruta inversos
- Relleno de credenciales

¿Cómo se pueden prevenir este tipo de ataques?, existen varias posibilidades que se deben implementar en las organizaciones para prevenir los ataques de fuerza bruta, algunas de las cuales son:

- Utilizar un nombre de usuario y una contraseña avanzada
- Elimina las cuentas no utilizadas con permisos de alto nivel
- Tasas de cifrado elevadas (256 bits)
- Salar el hash
- Autenticación de dos factores (2FA)
- Limitar el número de reintentos de inicio de sesión
- Bloqueo de la cuenta tras excesivos intentos de inicio de sesión
- Reduce el ritmo de los inicios de sesión repetidos
- Captcha obligatorio tras repetidos intentos de inicio de sesión
- Una lista de negación de IP para bloquear a los atacantes conocidos. (Karpersky, 2024)

Exfiltración de datos

La exfiltración de datos se trata básicamente del robo de datos, de acuerdo con IBM la definición exacta es la siguiente: “la exfiltración de datos, también conocida como extrusión o exportación de datos, es el robo de datos: la transferencia intencionada, no autorizada y

encubierta de datos desde una máquina a otro dispositivo, se puede realizar manualmente o automatizarse utilizando malware". (IBM, 2023)

Este tipo de ataques se encuentran entre las amenazas de ciberseguridad que son más destructivas y dañinas, esto independientemente del tipo y tamaño de la organización que pueda ser objeto de estos.

Para que un ataque de este tipo se materialice, deben existir los siguientes factores: un atacante externo (hacker, ciberdelincuente, adversario extranjero, etc.), una amenaza interna descuidada (un empleado, socio comercial, usuario autorizado que expone datos a través de un error humano, etc.).

Algunas de las técnicas más comunes de exfiltración de datos son las siguientes:

- Phishing
- Explotación de vulnerabilidades

Algunas de las consecuencias que puede generar la exfiltración de datos son las siguientes:

- Interrupción de las operaciones como consecuencia de la pérdida de datos cruciales para la empresa
- Pérdida de confianza de los clientes
- Secretos comerciales comprometidos, como desarrollos/invenciones de productos, códigos de aplicación únicos o procesos de fabricación.
- Graves multas reglamentarias, tasas y otras sanciones para las organizaciones
    - Ataques posteriores que puedan generarse por los datos exfiltrados. (IBM, 2023)

Estas son algunas de las acciones que se pueden tomar con el fin de prevenir este tipo de ataques:

- Formación de concienciación sobre seguridad
- Gestión de identidades y accesos (IAM): Autenticación multifactor, control de acceso basado en roles, autenticación adaptativa, inicio de sesión único.
- Prevención de pérdida de datos (DLP)
- Tecnologías de detección y respuesta a amenazas: sistemas de detección de intrusos (IDS), sistemas de prevención de intrusos (IPS), gestión de información y eventos de seguridad (SIEM), orquestación, automatización y respuesta de seguridad (SOAR), ejecución y detección de endpoints (EDR), soluciones de detección y respuesta extendidas (XDR). (IBM, 2023)

Ciclo de vida de la gestión de incidentes de ciberseguridad

La respuesta ante incidentes es el proceso mediante el cual una organización reacciona ante amenazas de TI, como es el caso de los ciberataques, las vulnerabilidades de seguridad y el tiempo de inactividad de los servidores.

El ciclo de vida de la respuesta ante incidentes es el marco de trabajo pormenorizado de una organización para identificar y reaccionar ante una interrupción del servicio o ante una amenaza de seguridad.

Los pasos del ciclo de vida de la respuesta ante incidentes son los siguientes de acuerdo con el NIST (National Institute of Standards and Technology) que es una agencia gubernamental que se encarga de establecer estándares y prácticas recomendadas sobre temas tales como la respuesta ante incidentes y la ciberseguridad, su campo de trabajo abarca todo tipo de cuestiones tecnológicas, entre las que se incluye la ciberseguridad, un ámbito en el que se han convertido en uno de los dos referentes estándares del sector en lo tocante a la respuesta ante incidentes gracias a su procedimiento de respuesta ante incidentes. (Atlassian, 2024)

El ciclo de vida de la respuesta ante incidentes según el NIST es el siguiente:

- Fase 1: Preparación

Abarca el trabajo que lleva a cabo una organización para prepararse para la respuesta ante incidentes, lo cual incluye el establecimiento de las herramientas y recursos adecuados y la capacitación del equipo.

- Fase 2: Detección y análisis

  Detectar y evaluar los incidentes con exactitud suele ser la parte más difícil de la respuesta ante incidentes para muchas organizaciones.

- Fase 3: Contención, erradicación y recuperación

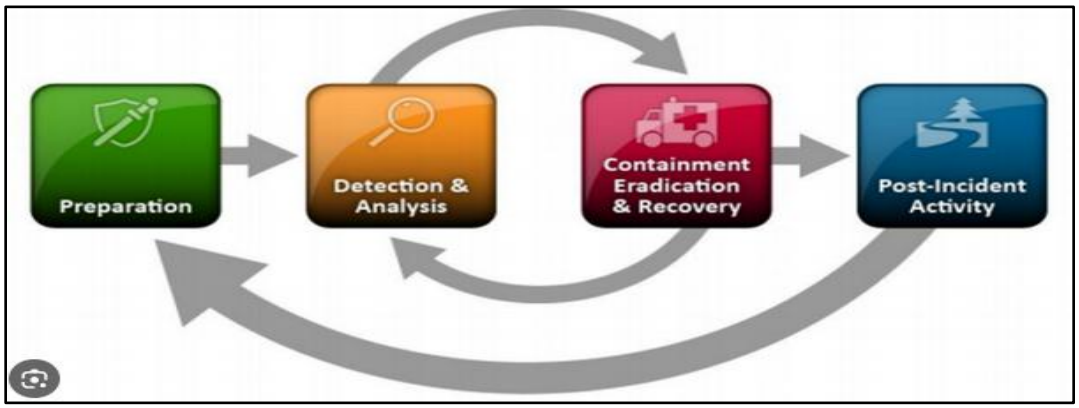
  Se centra en reducir al máximo las consecuencias del incidente y mitigar las perturbaciones del servicio.

- Fase 4: Actividad tras el evento

  Aprender y mejorar después de un incidente es uno de los componentes más importantes de la respuesta ante incidentes y el que más suele pasar por alto. En esta fase se analizan el incidente y los esfuerzos de respuesta correspondientes. Los objetivos son limitar las posibilidades de que el incidente vuelva a producirse e identificar formas de mejorar la actividad futura de respuesta ante incidentes.

Figura 7

Ciclo de vida NIST



Nota. Fuente: (AVSOFTWARE, 2023)

7. Tecnologías avanzadas en ciberseguridad

Extended detection and response (XDR)

Es una tecnología que representa la evolución de las soluciones de ciberseguridad tradicionales y ofrecen un enfoque más integrado y automatizado para la detección y respuesta ante amenazas. Conforme las ciberamenazas se vuelven más sofisticadas, la XDR proporciona un mecanismo de defensa integral que unifica múltiples capas de seguridad.

XDR está diseñado para abordar la complejidad de las amenazas modernas y las limitaciones de las medidas de seguridad tradicionales al ofrecer un enfoque unificado para la detección, investigación y respuesta ante amenazas. Integra datos de múltiples fuentes, como puntos finales, redes, entornos de nube, gestión de identidades y accesos y aplicaciones.

Algunos de los beneficios clave de la XDR incluyen:

- Capacidades de detección automatizada de amenazas
- Operaciones de seguridad optimizadas
- Tiempos de respuesta reducidos

- Postura de seguridad mejorada

XDR agrega datos de varias capas de seguridad, incluidos puntos finales, redes y entornos de nube. Aprovecha el aprendizaje automático y la inteligencia artificial para analizar esos datos en tiempo real e identificar patrones y anomalías que indican posibles amenazas.

Un ejemplo del uso de XDR es: un punto final detecta una actividad de inicio de sesión inusual mientras la capa de red registra intentos de exfiltración de datos, XDR correlaciona estos eventos para activar una respuesta automatizada.

El flujo de trabajo de XDR es el siguiente:

- Detección de incidentes: recopilación de datos unificada, integración de inteligencia sobre amenazas, enriquecimiento de datos, análisis avanzado.
- Análisis y puntuación del incidente: agrupación de alertas, puntuación del incidente, el incidente se puntúa según la gravedad de lo que XDR ha descubierto.
- Acciones de respuesta: veredicto malicioso, veredicto benigno.
- Monitoreo y mejora continua: monitoreo en tiempo real, análisis de amenazas inactivas, higiene y cumplimiento.

Los beneficios de XDR son los siguientes:

- Capacidades de detección y visibilidad mejoradas: son fundamentales, si las amenazas no se pueden ver, no se pueden identificar ni investigar y sobre todo no se pueden detener. XDR debe tener potentes capacidades de visibilidad y detección.
- Retención de datos: XDR recopila, correlaciona y analiza datos de la red, los puntos finales, la nube, la gestión de identidades y accesos y las aplicaciones

dentro de un único repositorio, que ofrece períodos personalizados de retención histórica.

- Análisis del tráfico interno y externo: la detección no puede buscar únicamente ataques que provengan de más allá del perímetro, sino que también debe perfilar y analizar las amenazas internas para buscar comportamientos anómalos y potencialmente maliciosos e identificar el uso indebido de credenciales.
- Inteligencia de amenazas integrada: la detección debe aprovechar la información sobre amenazas recopilada en una red global de empresas.
- Detección personalizable: deben ser altamente personalizables en función de las necesidades particulares de su entorno.
- Detección basada en aprendizaje automático: los ataques que no son detectados por los sensores en el punto final, la red o la nube deben descubrirse dentro de los datos de telemetría recopilados de estas fuentes y más allá. El aprendizaje automático es la única forma de procesar el gran volumen de datos de una organización empresarial.

Características propias de XDR:

- Integración de datos unificada
- Detección y respuesta automatizadas ante amenazas
- Análisis y correlación avanzados
- Análisis del comportamiento
- Visibilidad entre capas
- Búsqueda proactiva de amenazas
- Capacidades de respuesta integradas

- Escalabilidad y flexibilidad. (Paloaltonetworks, 2024)

Security Information and Event Management (SIEM)

De acuerdo con Microsoft SIEM es una solución de seguridad que ayuda a las organizaciones a detectar y analizar amenazas y responder a ellas antes de que afecten a las operaciones del negocio. Combina la administración de información de seguridad y la administración de eventos de seguridad en un solo sistema de administración de seguridad, esta tecnología recopila datos de registro de eventos de varias fuentes, identifica la actividad que se desvía de la norma con análisis en tiempo real y toma las medidas adecuadas.

Las herramientas SIEM recopilan, agregan y analizan volúmenes de datos de las aplicaciones, dispositivos, servidores y usuarios de una organización en tiempo real para que los equipos de seguridad puedan detectar y bloquear ataques.

Capacidades de los sistemas SIEM:

- Administración de registros: los sistemas SIEM recopilan grandes cantidades de datos en un solo lugar, los organizan y luego determinan si existen signos de amenaza, ataque o vulneración.
- Correlación de eventos: los datos se clasifican para identificar relaciones y patrones a fin de detectar amenazas potenciales y responder a ellas.
- Supervisión de incidentes y respuesta a ellos: la tecnología SIEM supervisa los incidentes de seguridad en la red de una organización y proporciona alertas y auditorías de toda la actividad relacionada con un incidente.

Ventajas de utilizar SIEM:

- Una visita centralizada de las amenazas potenciales

- Identificación y respuesta en tiempo real
- Inteligencia avanzada sobre amenazas
- Creación de informes y auditoría del cumplimiento normativo
- Una mayor transparencia a la hora de supervisar a los usuarios, las aplicaciones y los dispositivos.

Cómo implementar una solución SIEM:

- Definir los requisitos de la implementación de SIEM
- Hacer una serie de pruebas
- Recopilar suficientes datos
- Tener un plan de respuesta ante incidentes
- Seguir mejorando el SIEM. (MICROSOFT, 2024)

Intrusion detection systems (IDS)

De acuerdo con IBM, un sistema de detección de intrusos (IDS) es una herramienta de seguridad de red que monitoriza el tráfico y los dispositivos de la red en busca de actividades maliciosas conocidas, actividades sospechosas o infracciones de las políticas de seguridad. (IBM, 2022)

Un IDS puede ayudar a acelerar y automatizar la detección de amenazas en la red mediante alertas a los administradores de seguridad sobre amenazas conocidas o potenciales, o mediante el envío de alertas a una herramienta de seguridad centralizada.

Los IDS también pueden apoyar los esfuerzos de cumplimiento de la normativa, algunas de ellas como el estándar de seguridad de datos para la industria de tarjeta de pago (PCI-DSS), exigen que las organizaciones apliquen medidas de detección de intrusiones.

Actualmente suelen integrarse o incorporarse a los sistemas de prevención de intrusiones (IPS), que detectan las amenazas a la seguridad y actúan automáticamente para evitarlas.

Los sistemas de detección de intrusiones pueden estar aplicados en endpoints o unidades de hardware específicas conectadas a la red, algunas están disponibles como servicios en la nube.

Estos son los métodos utilizados por IDS:

- Detección basada en firmas: analiza los paquetes de red en busca de firmas de ataque, es decir características o comportamientos únicos asociados a una amenaza específica. Una secuencia de código que aparece en una variante de malware particular es un ejemplo de firma de ataque. Este tipo de IDS mantiene una base de datos de firmas de ataque con las que compara los paquetes de red, si un paquete coincide con una de las firmas, el IDS lo señala.
- Detección basada en anomalías: este tipo de métodos utilizan el machine learning para crear, y perfeccionar continuamente, un modelo de referencia de la actividad normal de la red luego compara la actividad de la red con el modelo y marca las desviaciones, como un proceso que utiliza más ancho de banda de lo normal o un dispositivo que abre un puerto.

Otros métodos de detección utilizados, pero menos comunes son los siguientes:

- Detección basada en la reputación: bloquea el tráfico procedente de direcciones IP y dominios asociados a actividades maliciosas o sospechosas.
- Análisis de protocolos con seguimiento de estado: se centra en el comportamiento del protocolo; por ejemplo, puede identificar un ataque de denegación de servicio (DDoS) detectando una única dirección IP que realiza muchas solicitudes de conexión de TCP simultáneas en un breve período de tiempo.

Existen varios tipos de sistemas IDS que se clasifican según su ubicación en el sistema y el tipo de actividad que supervisan:

- Sistemas de detección de intrusiones en la red (NIDS): monitorizan el tráfico entrante y saliente a los dispositivos a través de la red, se colocan en puntos estratégicos de la red, a menudo justo detrás de los firewalls en el perímetro de la red, para que puedan marcar cualquier tráfico malicioso que se abra paso.
- Sistemas de detección de intrusiones basado en host (HIDS): se instalan en un punto final específico, como un portátil, un router o un servidor. El HIDS solo supervisa la actividad en ese dispositivo, incluido el tráfico hacia y desde él, un HIDS suele funcionar tomando instantáneas periódicas de los archivos críticos del sistema operativo y comparando estas instantáneas a lo largo del tiempo, si el HIDS detecta un cambio, como la edición de archivos de registro o la alteración de configuraciones, alerta al equipo de seguridad.
- IDS basado en protocolos de aplicación (APIDS): funciona en la capa de aplicación, supervisando protocolos específicos de la aplicación, a menudo se despliega un APIDS entre un servidor web y una base de datos SQL para detectar inyecciones SQL.

Tácticas de evasión de IDS:

Estas son algunas de las tácticas más comunes de evasión de IDS:

- Ataques de denegación de servicio distribuido (DDoS): dejan fuera de línea a los sida, inundándolos con tráfico obviamente malicioso procedente de múltiples fuentes.

- Suplantación: falsificación de direcciones IP y registros de DNS para que parezca que el tráfico procede de una fuente fiable.
- Fragmentación: dividir el malware u otras cargas maliciosas en paquetes pequeños, ocultar la firma y evitar la detección. Retrasando estratégicamente los paquetes o enviándolos fuera de orden, los hackers pueden impedir que el IDS los vuelva a ensamblar y se percate del ataque.
- Cifrado: utilización de protocolos cifrados para omitir un IDS, si el IDS no tiene la clave de descifrado correspondiente.
- Fatiga del operador: genera un gran número de alertas IDS a propósito para distraer al equipo de respuesta a incidentes de su actividad real. (IBM, 2024)

Intrusion prevention systems (IPS)

Un Sistema de prevención de intrusiones (IPS) es un dispositivo de seguridad de red o una aplicación de software que supervisa el tráfico de la red y toma medidas automatizadas para evitar posibles amenazas y accesos no autorizados. Analiza el tráfico entrante y saliente, identifica la actividad maliciosa y toma medidas inmediatas para bloquear o mitigar las amenazas en tiempo real, salvaguardando la integridad y la seguridad de la red.

Este tipo de soluciones están automatizadas en gran medida, ayudan a filtrar la actividad maliciosa antes de que llegue a otros dispositivos o controles de seguridad, esto reduce el esfuerzo manual de los equipos de seguridad y permite que otros productos de seguridad funcionen de manera más eficiente.

Las soluciones IPS son eficaces para detectar y prevenir la explotación de vulnerabilidades, cuando se descubre una vulnerabilidad, suele haber una ventana de oportunidad para su explotación antes de que se pueda aplicar un parche de seguridad.

Los dispositivos IPS se diseñaron y lanzaron originalmente como dispositivos independientes a mediados de la década de los 2000, esta funcionalidad ha sido integrada en soluciones de gestión unificada de amenazas (UTM) y en firewalls de última generación, las nuevas soluciones IPS están conectadas a servicios de red y computación basados en la nube.

Estos sistemas funcionan de la siguiente manera: el IPS se coloca en línea, directamente en el flujo de tráfico de la red entre el origen y el destino. Esto es lo que diferencia el IPS de su predecesor, el sistema de detección de intrusiones (IDS), este por el contrario es ser un sistema pasivo que escanea el tráfico e informa sobre las amenazas.

La solución analiza todos los flujos de tráfico que ingresan a la red y toma acciones automatizadas cuando es necesario.

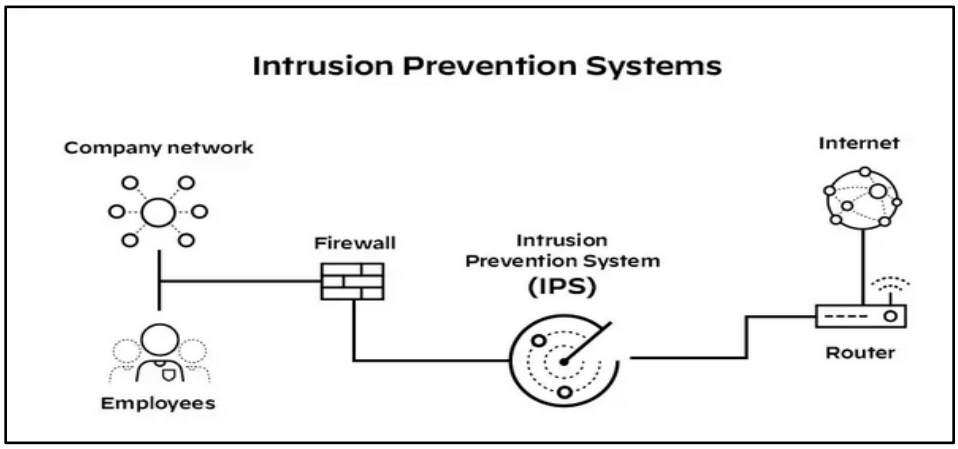
Algunas de estas acciones pueden incluir:

- Enviar una alarma al administrador
- Descartar los paquetes maliciosos
- Bloquear el tráfico desde la dirección de origen
- Restablecer la conexión
- Configuración de firewalls para prevenir futuros ataques

En la siguiente gráfica extraída de la web de PaloAlto Networks, se observa claramente la ubicación de un IPS en la infraestructura de la organización:

Figura 8

IPS



Nota. Fuente: (Paloaltonetworks, 2024)

Algunas de las técnicas utilizadas para utilizar de forma adecuada un IPS son las siguientes:

- Detección basada en firmas:

Es un método de detección basado en un diccionario de patrones (o firmas) identificables de forma única en el código de cada exploit, a medida que se descubre un exploit, su firma se registra y se almacena en un diccionario de firmas en constante crecimiento, esta detección se realiza de dos formas:

  - Firmas de vulnerabilidades de explotación
  - Firmas que detectan vulnerabilidades

- Detección basada en anomalías:

Toma muestras de tráfico de red al azar y las compara con un nivel de rendimiento de referencia calculado previamente, cuando la actividad del tráfico se encuentra fuera de los parámetros de rendimiento de referencia, el IPS toma medidas.

- Detección basada en políticas:

Requiere que los administradores de sistemas configuren políticas de seguridad en función de las políticas de seguridad y la infraestructura de red de una organización. Si se produce alguna actividad que infrinja una política de seguridad definida, se activa una alerta y se envía a los administradores.

Algunos de las soluciones de IPS más conocidas que existen son las siguientes:

- Sistema de prevención de intrusiones basado en red (NIPS)
- Sistema de prevención de intrusiones en el host (HIPS)
- El análisis del comportamiento de la red (NBA)
- El sistema de prevención de intrusiones inalámbricas (WIPS)

Los beneficios de los sistemas de prevención de intrusiones son:

- Riesgos comerciales reducidos y seguridad adicional
- Mejor visibilidad de los ataques y, por tanto, mejor protección
- Una mayor eficiencia permite la inspección de todo el tráfico en busca de amenazas
- Se necesitan menos recursos para gestionar vulnerabilidades y parches

Las principales características que debe tener un IPS son las siguientes:

- Protección contra vulnerabilidades de IPS
- Protección antimalware
- Protección integral de comando y control
- Acciones de seguridad automatizadas
- Visibilidad amplia y control granular
- Gestión de políticas consistente y simplificada
- Inteligencia de amenazas automatizada. (PALOALTONETWORKS, 2024)

Firewall de nueva generación (NGFW)

De acuerdo con Cisco, la definición de Firewall de nueva generación es la siguiente: “es un dispositivo de seguridad de red que ofrece funciones que van más allá de un firewall tradicional con estado. Si bien un firewall tradicional suele proporcionar una inspección con estado del tráfico de red entrante y saliente, un firewall de próxima generación incluye funciones adicionales como reconocimiento y control de aplicaciones, prevención de intrusiones integrada e inteligencia de amenazas en la nube.

Un firewall de última generación debe incluir lo siguiente:

- Capacidades de firewall estándar como inspección de estado
- Prevención de intrusiones integrada
- Conciencia y control de aplicaciones para ver y bloquear aplicaciones riesgosas
- Fuentes de inteligencia sobre amenazas
- Rutas de actualización para incluir fuentes de información futuras
- Técnicas para abordar las amenazas de seguridad en evolución

Algunas de las características principales que debe tener un firewall de próxima generación son las siguientes:

- Prevención de infracciones y seguridad avanzada:

  La función principal de un firewall debe ser evitar las infracciones y mantener segura a la organización, por este motivo debe tener capacidades avanzadas para detectar rápidamente malware avanzado si evade sus defensas de primera línea.

- Visibilidad integral de la red

  No se puede proteger contra lo que no se puede ver, es necesario supervisar lo que sucede en la red en todo momento para detectar comportamientos inadecuados y

detenerlos rápidamente, el firewall debe proporcionar una visión integral de la actividad y un conocimiento contextual completo.

- Opciones flexibles de gestión e implementación

  Independientemente de si tiene una empresa pequeña o mediana o una gran empresa, su firewall debe satisfacer sus necesidades específicas entre estas: administración para cada caso de uso, implemente en las instalaciones locales o en la nube a través de un firewall virtual.

- Tiempo de detección más rápido

  El tiempo estándar actual de la industria para detectar una amenaza es de entre 100 y 200 día, lo que es demasiado tiempo. Un firewall de próxima generación debería ser capaz de: detectar amenazas en segundos, detectar la presencia de una infracción exitosa en cuestión de horas o minutos, priorizar las alertas para tomar medidas rápidas y precisas para eliminar las amenazas, facilitar la vida implementando políticas consistentes y fáciles de mantener, con aplicación automática en todas las diferentes facetas de su organización.

- Automatización e integraciones de productos:

  Un firewall de próxima generación no debe ser una herramienta aislada, debe comunicarse y trabajar en conjunto con el resto de la arquitectura de seguridad, el firewall debe integrarse perfectamente con otras herramientas del mismo proveedor, compartir automáticamente información sobre amenazas, datos de eventos, políticas e información contextual con herramientas de seguridad de red, puntos finales, web y correo electrónico, automatizar tareas de seguridad como

evaluación de impacto, gestión y ajuste de políticas e identificación de usuarios. (CISCO, 2024)

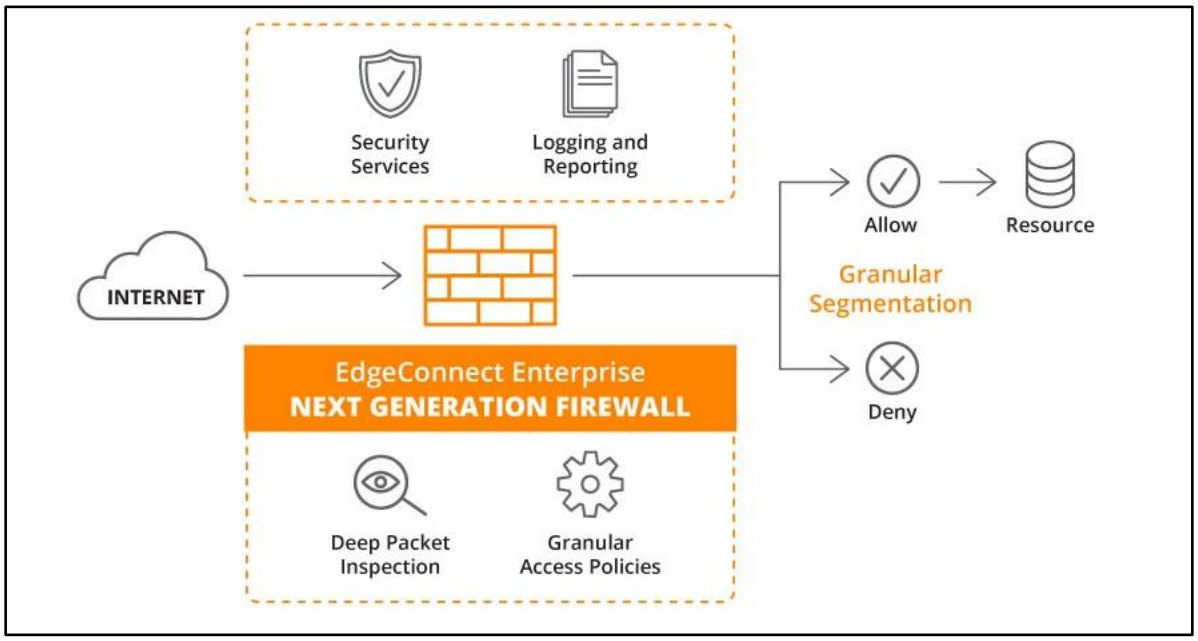
Los beneficios principales que tienen los NGFW, son los siguientes:

- App-ID: permite ver las aplicaciones en la red y aprender cómo funcionan, sus características de comportamiento y su riesgo relativo. Las aplicaciones se identifican a través de múltiples técnicas como las firmas de la aplicación, el descifrado (si se necesita), la decodificación del protocolo y la heurística.
- User-ID: identifica quienes son todos los usuarios en la red, no solo sus direcciones IP, mediante varias técnicas, métodos de acceso y sistemas operativos (Microsoft Windows, Apple iOS, Mac OS, Android y Linux) y asegura que se puedan detectar en todas las ubicaciones.
- Content-ID: combina un motor de prevención de amenazas en tiempo real con una completa base de datos de URL y elementos de identificación de la aplicación con el fin de limitar las transferencias de archivos y datos no autorizados, detectar y bloquear una amplia variedad de exploits, malware, navegación web peligrosa y amenazas desconocidas, recuperar el control sobre el tráfico de aplicaciones y contenido relacionado.

En la siguiente gráfica extraída de la web de arubanetworks (ARUBANETWORKS, 2024) se explica el funcionamiento de un NGFW:

Figura 9

Funcionamiento de un NGFW



En la siguiente gráfica también extraída de la web de arubanetworks se muestra una comparativa de los firewalls tradicionales versus los firewalls de nueva generación:

Figura 10

Comparativa de firewalls

Capacidad	Cortafuegos tradicional	NGFW	Ventajas de los NGFW
Inspección	Sin estado	Con estado	Bloquea el tráfico que se desvía de la norma esperada en comparación con las conexiones establecidas
Visibilidad	Rudimentaria, solo capas TCP/IP inferiores	Profunda, incluye todas las capas TCP/IP	Permite un análisis más granular y fiable del tráfico
Servicios	Básicos	Integrales	Incluye servicios de UTM como antivirus, filtrado de contenido, IDS/IPS o registro, además del filtrado de paquetes
Protección	Limitada	Mejorada	Identifica, previene e informa de una variedad más amplia de ataques

(ARUBANETWORKS, 2024)

Endpoint detection and response (EDR)

La definición de un EDR, de acuerdo con el Instituto Nacional de Ciberseguridad de España (incibe), es la siguiente: “es un sistema de protección de los equipos e infraestructuras de

una empresa, combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial para ofrecer una respuesta rápida y eficiente ante los riesgos y las amenazas más complejas". (incibe, 2024)

Debido a esta conjunción de elementos y tecnologías, permite detectar todos aquellos riesgos y amenazas que pueden provocar de forma silenciosa e inadvertida un incidente de seguridad, poniendo en riesgo la viabilidad de la empresa.

Un sistema EDR se caracteriza por unir varios elementos de detección y tecnologías, como, por ejemplo, la inteligencia artificial y el Big Data, que permiten mejorar de forma programada y autónoma la detección y prevención de amenazas complejas, así como su posterior eliminación o mitigación.

Aunque tiene algunas características de un antivirus tradicional, por ejemplo, la detección, identificación y la prevención de los efectos de malware, exploits, y en algunos casos, ransomware, esta herramienta además puede detectar amenazas avanzadas, como pueden ser malware de tipo polimórfico, vulnerabilidades 0-day, ataques de ingeniería social, amenazas persistentes o APT, cuentas comprometidas, etc. Cuando se detecta una amenaza o comportamiento anómalo, permite actuar de forma inmediata y casi automática para eliminar la amenaza o mitigar sus efectos.

Algunas otras características que tienen los EDR son las siguientes:

- Herramientas de análisis apoyadas en el uso del aprendizaje automático (machine learning) para mejorar la detección de amenazas
- Sandbox: el sistema virtual y aislado de pruebas para comprobar el comportamiento de los archivos descargados, entre otras cosas.

- Escaneo de IOCs y reglas YARA, que permiten analizar y detectar las amenazas provocadas por amenazas complejas en tiempo real.
- El uso de listas blancas y negras de correos electrónicos, páginas web e IP.
- Interoperabilidad e interacción con otras herramientas de seguridad, como SIEM, IPS/IDS o herramientas antimalware.

Como todo producto tecnológico los EDR tienen sus ventajas y desventajas, a continuación, se detallan algunas de ellas:

Ventajas:

- Recopila información exhaustiva y detallada de las características del dispositivo, como información del sistema operativo, del hardware o los procesos activos, entre otros datos.
- Permite recopilar y almacenar información de forma automática, así como crear patrones de detección automatizados, facilitando el trabajo de detección.
- Monitoriza la integridad de los sistemas y de los archivos de configuración claves, avisando en caso de modificación o acceso a estos por actores sospechosos.
- Permite localizar en un solo punto toda la información, posibilitando en caso de incidente la realización de una investigación de forma rápida.

Desventajas:

- En algunos casos no permite evaluar y comprobar aquellos dispositivos con sistemas operativos no soportados por la herramienta.
- Su configuración y puesta en marcha es más complicada de realizar que en el caso de un antivirus tradicional.

- Su uso puede provocar fatiga, debido al constante flujo de información y notificación de las propias alertas configuradas, así como de los falsos positivos y negativos que pueden darse.
- En ocasiones no permite monitorizar y analizar las conexiones cifradas.
- La inversión para implementar esta herramienta supone un importe más elevado que en el caso de un antivirus tradicional o EPP.

Un EDR puede tener un gran impacto en la respuesta a incidentes, pues ayuda a los equipos respectivos a generar eficiencias en cada fase de sus planes de respuesta a incidentes, además de que les ayudan a detectar amenazas que de otro modo podrían permanecer invisibles, los EDR pueden aliviar las tareas manuales y tediosas asociadas con las últimas fases del ciclo de vida de la respuesta a incidentes, a saber:

- Contención, erradicación y recuperación
- Análisis posterior al evento

Security orchestration, automation, and response (SOAR)

El SOAR describe un conjunto de funciones que se utilizan para proteger los sistemas de TI de las amenazas. Hace referencia a tres funciones clave del software que utilizan los equipos de ciberseguridad: la gestión de los casos y los flujos de trabajo; la automatización de las tareas y un método centralizado para acceder a la información sobre las amenazas, consultarla y compartir los datos sobre ella.

Las herramientas de tipo SOAR se suelen implementar en colaboración con el Centro de Operaciones de Seguridad de las empresas (SOC), las plataformas que emplean este concepto pueden supervisar las fuentes de información sobre amenazas y generar respuestas automáticas

para mitigar los problemas de seguridad. De esta forma, los equipos de TI reducen las amenazas de forma rápida y eficiente en muchos sistemas complejos. (RedHat, 2024)

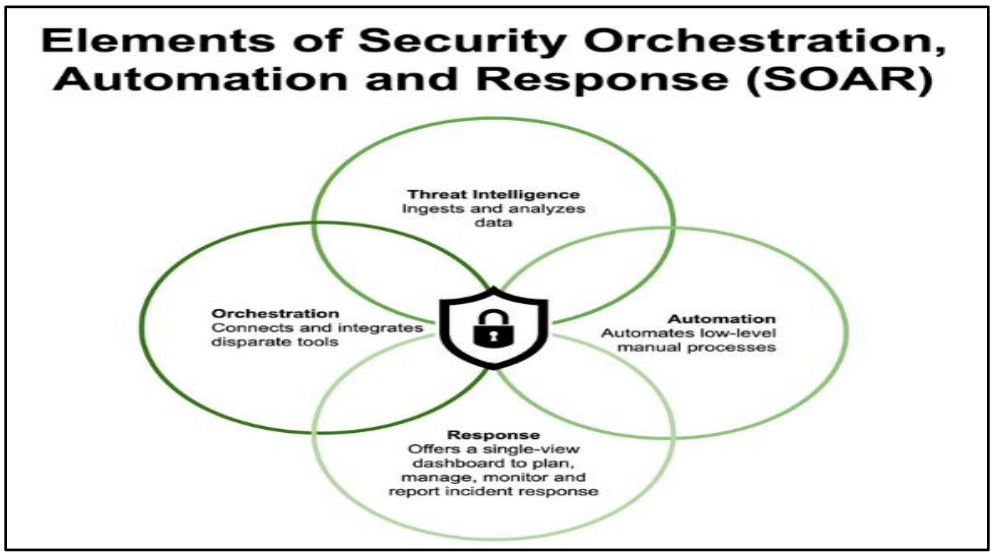
Algunos de los beneficios de SOAR son los siguientes:

- Procesando más alertas en menos tiempo: las SOC pueden tener que lidiar con cientos o miles de alertas de seguridad diariamente, esto puede generar fatiga ante las alertas y los analistas pueden pasar por alto señales importantes de actividad de amenazas, los SOAR pueden hacer que las alertas sean más manejables al centralizar los datos de seguridad, enriquecer los eventos y automatizar las respuestas.
- Planes de respuesta a incidentes más consistentes: los SOC pueden utilizar los manuales SOAR para definir flujos de trabajo de respuesta a incidentes estándar y escalables para amenazas comunes.
- Toma de decisiones mejorada del SOC: los SOC pueden utilizar los paneles de SOAR para obtener información sobre sus redes y las amenazas a las que se enfrentan, esta información puede ayudar a los SOC a detectar falsos positivos, priorizar mejor las alertas y seleccionar los procesos de respuesta correctos.
- Colaboración mejorada del SOC: los SOAR centralizan los datos de seguridad y los procesos de respuesta a incidentes para que los analistas puedan trabajar juntos en las investigaciones.

En la siguiente gráfica extraída de paloaltonetworks se observa los elementos propios de un SOAR:

Figura 11

Elementos de un SOAR



(paloaltonetworks, 2024)

ServiceNow

Se define como un sistema de acción, una plataforma que se ubica por sobre los datos y los sistemas existentes de las organizaciones, lo que evita la necesidad de copiar y reemplazar esos sistemas existentes. Con interfaces simples y fáciles de usar que facultan a los empleados y los clientes la capacidad de organizar y automatizar deliberadamente las tareas y los procesos en todas sus empresas, lo que también se extiende a sus ecosistemas.

De acuerdo con la web de servicenow.com este producto tiene dos décadas como parte integral del mundo de la TI, fundado en 2004. La idea inicial fue crear una plataforma basada en la nube para un trabajo de enrutamiento de manera eficaz que fuera lo suficientemente bueno para impulsar el éxito empresarial, pero simple a fin de no espantar a posibles usuarios.

Algunas de las soluciones que proporciona ServiceNow son:

- Excelencia en tecnología

- Experiencia del cliente
- Excelencia operativa
- Experiencia de los empleados
- Hiperautomatización y código simple
- Gestión de la cadena de suministros y finanzas

Los beneficios de tener ServiceNow son los siguientes:

- Experiencias simplificadas
- Automatización con intención
- Agilidad organizacional

En el campo de la TI, ServiceNow desempeña un rol principal en las telecomunicaciones, los medios y la tecnología, lo que permite a las organizaciones de estos sectores gestionar infraestructuras de TI complejas e impulsar la innovación de manera más eficaz.

Algunas de las empresas más reconocidas que utilizan esta tecnología son las siguientes:

- Accenture
- Deloitte
- Ciudad de Copenhague
- 7-Eleven

Estos son algunos de los productos de ServiceNow que se encuentran disponibles:

- IT Service Management (ITSM)
- IT Operations Management (ITOM)
- Customer Service Management (CSM)
- App Engine
- Automation Engine

- Strategic Portfolio Management (SPM)
- HR Service Delivery
- Security Operations (SecOps)
- Governance, Risk and Compliance (GRC)
- Workplace Service Delivery (WSD)
- Field Service Management (FSM)
- Cadena de suministros y finanzas

Splunk

Splunk es una herramienta de Cisco, de acuerdo con la web de splunk se define de la siguiente forma: “es una plataforma de Big Data que puede ayudarle a hacer muchas cosas mejor, su uso correcto potencia la ciberseguridad, la observabilidad, las operaciones de red y una gran cantidad de tareas importantes que requieren las grandes organizaciones”. (Splunk, 2024)

Las organizaciones que utilizan Splunk pueden enfrentar las disrupciones digitales de una manera diferente, ofreciendo una visibilidad integral, detección e investigación rápidas y recursos optimizados.

Splunk se compone de un conjunto completo de software, aplicaciones y API, entre los productos más conocidos se encuentran los siguientes:

- Splunk Enterprise
- Splunk Cloud Platform
- Reenvío universal
- Splunk Enterprise Security
- Soluciones SOAR

Algunas de las funciones principales que tiene Splunk son las siguientes:

- Supervisar, buscar, indexar y correlacionar datos de una variedad de fuentes
- Buscar, analizar grandes datos, configura alertas, informes y visualizaciones relevantes
- Potencia las operaciones de ciberseguridad, desde la respuesta y gestión de incidentes hasta la detección y búsqueda de amenazas
- Hace que el cumplimiento y la presentación de informes sea muy sencillo.
- Ayuda a obtener la visibilidad completa de las operaciones comerciales y de TI.

Splunk es una plataforma de análisis de datos en tiempo real que permite supervisar y analizar toda la infraestructura de TI. Esto incluye desde servidores y aplicaciones hasta dispositivos de red, base de datos y servicios en la nube. También ofrece características como la capacidad de profundizar en áreas específicas de interés, crear dashboards personalizados en función de sus necesidades y generar informes que se pueden compartir con otros usuarios como business intelligence.

Splunk consta de 3 componentes esenciales:

- El indexador: recibe los datos de las diferentes fuentes y los almacena en una base de datos interna
- Componente inicial de búsqueda: filtra solo la información que es necesaria antes de enviarla de nuevo al indexador para su almacenamiento.
- Consola de análisis que permite ver los resultados, crear visualizaciones y realizar búsquedas avanzadas.

Las ventajas que tiene Splunk son las siguientes:

- Buena flexibilidad en sus opciones de despliegue puede ser desplegado onpremise o en Cloud de acuerdo con las necesidades.

- Ayuda a ahorrar tiempo y dinero al reducir el número de personas necesarias para realizar tareas de monitorización.
- Proporciona capacidades de monitorización en tiempo real, lo que significa que será posible actuar sobre alguna alerta de inmediato en lugar de tener que esperar hasta más tarde.
- Se pueden realizar análisis avanzados para cualquier tipo de recopilación de datos.
- Se pueden realizar visualizaciones que permiten ver las tendencias y los patrones visualmente antes de realizar cualquier otro tipo de análisis en sus datos.

Desventajas:

- Ocupa más espacio que otras soluciones.

La implementación de Splunk implica varios pasos y procesos, como planificar y diseñar el entorno, instalar y configurar el software, integrar con otras herramientas y sistemas, monitorizar y administrar el rendimiento y la salud del sistema, y realizar tareas de mantenimiento y actualización regularmente.

Puede ser administrado e implementado por un equipo de TI experimentado o con la ayuda de un proveedor de servicios.

Splunk puede ser una herramienta costosa y compleja de implementar y administrar, y puede requerir una buena planificación y ejecución para asegurarse de que el sistema pueda manejar una gran cantidad de datos y usuarios.

8. Automatización en Ciberseguridad

Concepto

La empresa IBM en su página web define la automatización de la siguiente forma: “la automatización es la aplicación de tecnología, programas, robótica o procesos para lograr resultados con una intervención humana mínima”. (ibm, 2022)

El software y las tecnologías de automatización se emplean en una amplia gama de industrias, desde finanzas hasta atención médica, servicios públicos y defensa, y prácticamente en todas partes intermedias.

Las organizaciones emplean la automatización para aumentar la productividad y la rentabilidad, mejorar el servicio y la satisfacción del cliente, reducir costos y errores operativos, cumplir las normas, optimizar la eficacia operativa y mucho más. La automatización es un componente clave de la transformación digital y es invaluable para ayudar a las empresas a escalar.

Existen tres tipos de automatización, a saber:

- Automatización básica: automatiza tareas simples y rudimentarias, se trata de digitalizar el trabajo mediante el uso de herramientas para agilizar y centralizar las tareas rutinarias, como utilizar un sistema de mensajería compartida en lugar de tener información en silos inconexos.
- Automatización de procesos: gestiona los procesos empresariales para lograr uniformidad y transparencia, por lo general se administra mediante software dedicado y aplicaciones empresariales, su uso puede aumentar la productividad y la eficiencia en su negocio.
- Automatización inteligente: es donde las máquinas pueden imitar las tareas humanas y repetir las acciones una vez que los humanos definen las reglas para la máquina.

Herramientas de automatización de ciberseguridad

Con la digitalización existente en las organizaciones actualmente, es muy importante mantener la seguridad de los sistemas informáticos, pues esto provoca la aparición constante de nuevas vulnerabilidades en todo tipo de software y servicios, y esto suele ser aprovechado por los ciberatacantes para aprovechar estas brechas de seguridad con la mayor rapidez.

Debido a esto el escaneo de vulnerabilidades es un proceso clave para reforzar la ciberseguridad de los sistemas y conocer en detalle el estado de la seguridad de la infraestructura en una organización.

El escaneo de vulnerabilidades es una técnica en ciberseguridad que involucra la identificación y evaluación de los servicios y aplicaciones de una infraestructura, con el objetivo de encontrar posibles puntos débiles en los sistemas de una red. (OpenWebinars, 2024)

En este proceso se examinan redes, aplicaciones y sistemas informáticos, con el objetivo de detectar fallas de seguridad que podrían ser explotadas por los ciberatacantes. Algunas de las vulnerabilidades encontradas pueden ser desde problemas de software desactualizado, configuraciones incorrectas, falta de medidas de seguridad adecuadas, entre otros. (OpenWebinars, 2024)

Realizando estos escaneos se puede obtener una radiografía detallada de la salud de seguridad de la infraestructura de red en una empresa en un período de tiempo determinado. Es por eso por lo que se recomienda realizar escaneos de vulnerabilidades de forma periódica, para detectar nuevas amenazas y vulnerabilidades. (OpenWebinars, 2024)

Los objetivos principales del escaneo son los siguientes:

- Detección de vulnerabilidades: identificar puntos débiles en el software, hardware o en las configuraciones de red que podrían ser explotadas por actores maliciosos.

- Clasificación y priorización: evaluar el nivel de riesgo de cada vulnerabilidad detectada, ayudando a determinar qué problemas deben abordarse primero para atacar las vulnerabilidades más críticas a la mayor brevedad posible.
- Preparación para acciones correctivas: los escaneos proporcionan información valiosa para mitigar o eliminar las vulnerabilidades encontradas, contribuyendo a aumentar la seguridad de la red. (OpenWebinars, 2024)

Existen varios tipos de escaneo de vulnerabilidades que se pueden realizar, y para esto diferentes tipos de herramientas, se detallan los siguientes:

- Escaneo de red
- Escaneo de aplicaciones web
- Escaneo de sistemas operativos y software

A continuación, se van a detallar algunas de las herramientas existentes en el mercado para realizar escaneos de vulnerabilidades con sus principales características:

NMap

Network Mapper, es una herramienta ampliamente utilizada en el ámbito de la seguridad informática para el descubrimiento de redes y la detección de vulnerabilidades en los servicios detectados gracias a sus scripts.

Algunas de sus características son:

- Gran detección de puertos y servicios
- Reconocimiento de red
- Flexibilidad para escanear

Normalmente se utiliza mediante línea de comandos, aunque existe una interfaz gráfica llamada Zenmap, que se encuentra disponible en plataformas como Linux, Windows y Mac.

Nessus

Es una de las herramientas de escaneo de vulnerabilidades más populares y confiables, conocida por su gran potencia de escaneo y la gran cantidad de información que puede encontrar con sus distintos modos de detección.

Algunas de sus características principales son las siguientes:

- Amplia cobertura de vulnerabilidades: es conocida por su gran base de datos de vulnerabilidades, pudiendo identificar vulnerabilidades de infraestructuras al completo.
- Interfaz de usuario amigable: posee una interfaz intuitiva que facilita su uso y organiza la información de las vulnerabilidades descubiertas de forma práctica, además, la organización de los escaneos.
- Alta capacidad de configuración: dispone de una gran variedad de parámetros para configurar los escaneos, de forma que se adapten al máximo a la infraestructura a escanear.

OpenVAS

Es una solución de escaneo de vulnerabilidades de código abierto con capacidad de integrarse con distintas plataformas de monitorización de sistemas y seguridad. Entre sus características principales se encuentran:

- Escaneo integral y granular: es capaz de escanear una amplia variedad de servicios y redes, con capacidad de ajustar la amplitud y profundidad de la detección en los sistemas.

- Actualizaciones constantes: contiene una base de datos de vulnerabilidades se actualiza regularmente, lo que garantiza la detección de las amenazas más recientes.
- Flexibilidad y escalabilidad: admite una variedad de sistemas operativos IT y OT, y permite una gran escalabilidad, capaz de escanear grandes redes de forma eficiente.

Qualys

Qualys es un proveedor líder y pionero de soluciones de cumplimiento y seguridad en la nube. Se basa en soluciones de cumplimiento y seguridad, ayuda a racionalizar y consolidar las soluciones de seguridad y cumplimiento desde una única plataforma y añadir seguridad en las iniciativas de transformación digital para una mayor agilidad.

Cuenta con una herramienta denominada VMDR, lo que es un ciclo de protección continuo desde un solo lugar, con flujos de trabajo de coordinación integrados y detección de vulnerabilidades en tiempo real, con el fin de priorizar, remediar y auditar en entornos de TI híbridos, que combinan componentes de la nube con componentes físicos.

Algunas de las ventajas principales con las que cuenta Qualys VMDR son las siguientes:

- Posibilita la gestión de vulnerabilidades y ofrece a los equipos de TI una visibilidad completa y continua de sus activos de TI globales.
- Identifica vulnerabilidades en todos los activos en tiempo real.
- Prioriza la remediación mediante aprendizaje automático y conciencia de contexto
- Proporciona flujos de trabajo de orquestación integrados
- Permite la remediación mediante un click con rastreo completo para auditorías.

VMDR agrupa funciones de detección de activos, inventario y evaluación de vulnerabilidades, e incluye controles de configuración, priorización, remediación y auditoría en una única app.

Ventajas de la Automatización

Cuando se tienen las herramientas adecuadas, la automatización de procesos en TI puede ser sorprendentemente fácil y puede ofrecer beneficios importantes, entender estos beneficios ayudará a la organización a tener una base sólida para implementar un proyecto de automatización de procesos.

Los beneficios principales que se han citado comúnmente en cuanto a la utilización de un centro de datos automatizado o desatendido son las siguientes:

Reducción de costos: un software de automatización es un enfoque mejor y más inteligente para contener y reducir costos, la oportunidad más grande que presenta es la de aumentar el servicio al cliente (usuario final) mientras que se reducen los costos sistemáticamente.

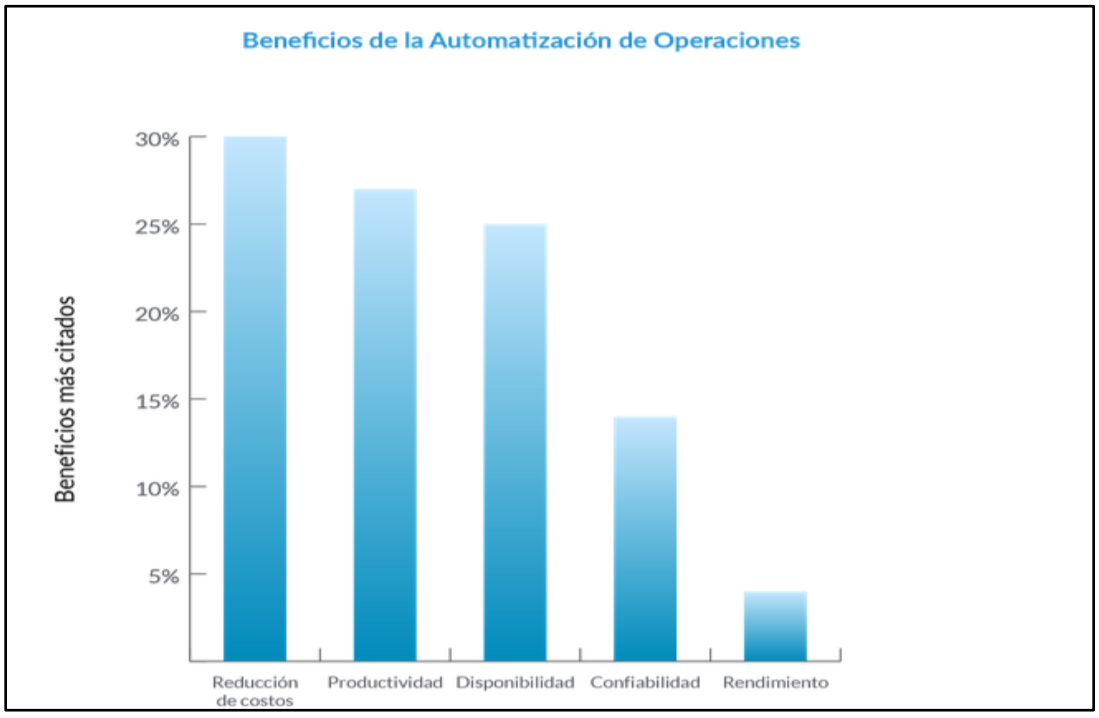
- Aumento de la productividad: un software de optimización de procesos puede resolver estos inconvenientes de muchas formas, se optimiza el rendimiento al automatizar la programación de los lotes en producción.
- Disponibilidad: la alta disponibilidad es claramente uno de los objetivos principales de los departamentos de TI, la posibilidad de automatizar sistemas de guardado y recuperación para garantizar la protección contra potenciales desastres, como la pérdida de disco, o daños inadvertidos a los objetos del sistema causados por un error humano, es una de las mayores ventajas de la automatización.

- Confiabilidad: la confiabilidad es la piedra angular de cualquier buen departamento de operaciones de TI, los procesos automatizados aseguran que los trabajos no sean olvidados ni se ejecuten fuera de secuencia, que los datos que se ingresen sean correctos, y que se realice cualquier procesamiento especial que sea necesario.
- Rendimiento: un software de automatización puede resolver los desafíos de rendimiento y ayuda a aumentar el rendimiento de los sistemas.

En la siguiente imagen obtenida de la web fortra.com se puede observar gráficamente el resultado de la afirmación anterior:

Figura 12

Beneficios de la automatización



Nota. Fuente: (Fortra, 2024)

Desventajas y obstáculos de la automatización de procesos

La automatización de procesos a pesar de contar con una gran cantidad de ventajas es un proceso que no resulta sencillo de implementar, pues existen muchas trampas y obstáculos que se deben superar.

En las organizaciones siempre se encuentran excusas para no realizar alguna tarea necesaria para dar pie con la automatización, de acuerdo con la web fortra.com en una reciente encuesta realizada en la cual se le consultó a diferentes empresas por qué no se habían automatizado sus sistemas, las empresas encuestadas respondieron en un 43 % que habían agregado e identificado proyectos de automatización a sus calendarios, es decir, un 57 % de las compañías no habían reconocido los beneficios potenciales de esta tecnología.

Los obstáculos se dividen en dos categorías:

- Costo
- Personas

En cuanto a las desventajas de la automatización de los procesos se cuenta con las siguientes:

- Alta inversión inicial: la implementación de procesos automatizados implica una inversión significativa en tecnología, software y hardware especializado, esta inversión puede ser una barrera para las empresas pequeñas y medianas que pueden no contar con los recursos financieros necesarios para adoptar estas soluciones.

- Dependencia de la tecnología: estos procesos dependen en gran medida de la tecnología, cualquier falla en los sistemas, ya sea por problemas técnicos, cortes de energía o ciberataques, puede detener por completo la operación de la empresa.
- Desplazamiento de empleados: con la automatización de las tareas es posible que algunas funciones y puestos de trabajo sean redundantes, esto puede llevar a la reubicación o reentrenamiento de los empleados, o en algunos casos, a la reducción de la fuerza laboral.
- Posibles errores en la implementación: si los procesos automatizados se diseñan de manera inadecuada, los errores pueden replicarse a gran escala antes de ser detectados y corregidos, esto puede generar problemas significativos.
- Falta de flexibilidad: algunos de estos sistemas pueden carecer de la flexibilidad necesaria para adaptarse a cambios en los procesos del entorno empresarial, esto a su vez puede afectar a la empresa para adaptarse a nuevas demandas o desafíos inesperados.

Ansible

La web de RedHat definde Ansible como: “un motor open source que automatiza una gran cantidad de procesos informáticos, como la preparación de la infraestructura, la gestión de la configuración, la implementación de las aplicaciones y la organización de los sistemas.” (RedHat, 2022)

Esta herramienta se puede utilizar para instalar software, automatizar tareas cotidianas, preparar elementos de infraestructura y de red, mejorar la seguridad y el cumplimiento normativo, aplicar parches a los sistemas y organizar flujos de trabajo complejos.

Ansible se conecta a los nodos o hosts y les inserta pequeños programas denominados módulos, los nodos son los extremos objetivo (servidores, dispositivos de red, o computadoras) que se desean gestionar con la plataforma. Los módulos son utilizados para realizar tareas de automatización en Ansible. Estos programas se escriben para que sean modelos de los recursos del estado deseado del sistema, luego Ansible los ejecuta y los elimina al finalizar.

Una de las características principales de Ansible es que no necesitan agentes, por lo tanto, no es necesario instalar ningún software en los nodos que gestiona. La plataforma lee la información del inventario para saber qué máquinas desea gestionar.

La plataforma se conecta a los servidores utilizando el protocolo SSH, y de esta misma forma ejecuta las tareas. Ansible utiliza claves y agentes de SSH para conectarse a las máquinas remotas con el nombre de usuario actual, no se debe iniciar sesión como un superusuario, sino que puede hacerlo como cualquier otro y luego utilizar los comandos necesarios para adquirir nuevos privilegios.

Algunos de los beneficios de la automatización con Ansible son los siguientes:

- Reduce los recursos necesarios para la gestión de TI: los Sysadmins pueden contener cientos o incluso miles de máquinas desde un único punto y de una sola vez.
- Hace accesible la automatización: uno de los objetivos de Ansible fue que se requiriera un aprendizaje mínimo de uso, es fácil porque YAML es un lenguaje legible para personas con elementos de otros idiomas de programación.
- No afecta al rendimiento: no requiere agentes, ni software, ni recursos informáticos que se ejecute o instale en sistemas gestionados.

- Garantiza la coherencia: la plataforma se diseñó para ser mínima y permitir a los usuarios crear entornos coherentes, además, como toda la operación se realiza a través de una conexión SSH, no añade más complejidad a los sistemas.

Puppet

Puppet es una herramienta de infraestructura como código (IaC), basada en convergencia y con un modelo push-and-pull que utiliza el lenguaje declarativo Puppet para describir el estado deseado de la infraestructura.

Normalmente administra sistemas mutables, lo que significa que se administra su configuración durante todo su ciclo de vida en lugar de reconstruirlos desde cero en cada cambio de configuración, como se haría con los contenedores Docker por ejemplo. Puppet se utiliza principalmente pero no exclusivamente, para administrar NIX y Windows a nivel de sistema operativo.

Una implementación tradicional de Puppet basada en extracción consta de uno o más servidores Puppet y un agente Puppet en cada sistema (nodo) que se administra. Los agentes consultan los servidores para obtener el último estado deseado como catálogo para el nodo en el que se están ejecutando. Si hay alguna diferencia con respecto al estado deseado, el agente que se ejecuta con privilegios de root soluciona la situación.

Algunas de las ventajas de Puppet son las siguientes:

- Entrega de continua de cambios de configuración sin un sistema CI/CD dedicado.
- Aplicación continua de políticas: los agentes garantizan que los sistemas cumplan con las políticas definidas.

- Transportes TLS confiable: no es necesario preocuparse por problemas clave de host o de hosts conocidos que tiene SSH.
- Los nodos administrados solo tienen acceso a su propio código.
- Se escala bien a miles de nodos administrados.

La forma de trabajar de Puppet es la siguiente: cuando se aplica el código Puppet a un nodo, primero se compila el código en un catálogo, que es una descripción del estado deseado. El catálogo no contiene ninguna lógica condicional, pues las condiciones se resuelven en función de las variables y los hechos que se pasan al compilador del catálogo. La aplicación del estado deseado se produce en el nivel de recursos (paquetes, archivos, servicios).

Chef

De acuerdo con IBM, la definición de Chef es la siguiente: “es una herramienta de gestión de configuración de código abierto que puede utilizar para crear partes de una infraestructura como servicio (IaaS)”. (IBM, 2022)

Los scripts de Chef, que son conocidos como recetas, están hechos de definiciones reutilizables que se escriben en el lenguaje de programación Ruby. Estas recetas se agrupan en un único contenedor, denominado libro de cocina. Los recetarios y las recetas automatizan tareas de infraestructura comunes.

Algunas de las ventajas principales de utilizar Chef son las siguientes:

- Reduce errores manuales e inconsistencias
- Aumenta la eficiencia y productividad mediante la automatización de tareas complejas
- Mejora la escalabilidad y flexibilidad
- Fomenta la colaboración y la innovación

- Permite aprovechar las mejores prácticas de la comunidad de chefs.

En cuanto a los desafíos y limitaciones de usar Chef están los siguientes:

- Se deben tener conocimientos de Ruby y Chef DSL.
- Puede ser lento y consumir muchos recursos en entornos de infraestructuras grandes y complejos.
- La solución de problemas y la depuración con Chef pueden ser difíciles cuando algo sale mal en los nodos o servidores.
- Chef puede ser incompatible o inconsistente con sistemas operativos, plataformas o aplicaciones que tienen sus propios sistemas de configuración y administración.

9. Metodologías ágiles en ciberseguridad

Los procesos ágiles en tecnología son procesos de negocios que permiten alcanzar alguno de los objetivos de negocio de la organización y que son automatizados en un sistema de gestión de procesos de negocios siguiendo los principios de las metodologías ágiles de desarrollo de software.

La mayoría de las metodologías de desarrollo ágiles de software se basan en los siguientes conceptos:

- Lista de Pendientes, donde se listan las tareas a realizar.
- Planificación, donde se priorizan y asignan responsables para las tareas
- Tarjetas (Cards), que permiten dar seguimiento a las tareas y su avance.
- Construcción (1 a 3 semanas, con reuniones diarias o daylis), donde se realizan las tareas
- Entrega de producto, cuando se evalúa si el producto está terminado para el cliente, o se debe reiniciar un nuevo ciclo.

- Reunión de revisión, en la que se extraen aprendizajes para el siguiente proyecto.

La automatización de flujos de trabajo ágiles es factible aplicando los principios generales de las metodologías ágiles de proyectos de software. Para esto es clave contar con un sistema de gestión de procesos de negocios low-code/no-code, que no requieren programación y permita ciclos iterativos cortos.

Principios de las metodologías ágiles

Las metodologías agiles se basan en 12 principios que se detallan a continuación:

- Satisfacer al cliente mediante la entrega temprana y continua: la satisfacción del cliente, así como una entrega pronta y frecuente de software valioso son fundamentales para conseguirla, al incrementar las posibilidades de satisfacer las demandas de los clientes y propiciar un retorno de la inversión más rápido.
- Aprovechar el cambio como ventaja competitiva: esto se logra aceptando modificaciones en los requisitos hasta en las últimas fases de un proyecto, aprovechar los cambios aportará al cliente una ventaja competitiva, pues atenderá a las necesidades actuales de los usuarios.
- Entregar valor frecuente: se refiere a la necesidad de entregar actualizaciones del software más pequeñas cada menos tiempo, este tipo de entregas requieren menos tiempo de planificación y reducen las posibilidades de que se produzcan errores en su desarrollo, además, más entregas se traducen en más feedback por parte del cliente.
- Cooperación negocio-desarrolladores durante todo el proyecto: se propone poner fin a las barreras existentes entre los equipos de negocio y de desarrollo de

software, para mejorar la comprensión y la colaboración entre ambas partes y conseguir mejores resultados.

- Construir proyectos en torno a individuos motivados: la idea es motivar y potenciar a los miembros del equipo de desarrollo para que se sientan motivados, para que sean capaces de llevar a cabo los proyectos de mejor forma.
- Utilizar la comunicación cara a cara: se potencia este tipo de comunicación, pues es la más adecuada para llevar a cabo proyectos de forma exitosa, es la más efectiva, ya que reduce de forma notable los tiempos de respuesta y los malentendidos.
- Software funcionando como medida de progreso: es una medida fundamental para que las organizaciones conozcan el progreso de un proyecto y esto es el software en funcionamiento.
- Promover y mantener un desarrollo sostenible: todas las partes involucradas en el proceso de desarrollo de software deben mantener un ritmo que pueda ser seguido por todos ellos, evitando tensiones o presiones excesivas.
- La excelencia técnica mejora la agilidad: cuidar los aspectos técnicos a la hora de desarrollar un producto de software aporta agilidad, será más sencillo ir actualizando el software cuando sea necesario si se ha construido cuidadosamente y cuenta con un buen diseño, que si no se ha hecho.
- La simplicidad es fundamental: actuar de la forma más sencilla posible, el cliente no paga por el esfuerzo realizado, sino porque se le entregue una solución que atienda a sus necesidades.

- Equipos auto-organizados para generar más valor: los equipos a los que se les da una libertad y una confianza suficientes son los que consiguen los mejores resultados.
- Reflexión y ajustes frecuentes del trabajo de los equipos: los equipos deben revisar frecuentemente su trabajo, para ajustarlo y mejorar su rendimiento.

Agilidad en proyectos de ciberseguridad

Las metodologías ágiles se basan en principios de colaboración, adaptación y flexibilidad, y se enfocan en crear software de alta calidad de manera más rápida y eficiente.

Desde este punto de vista existen dos pilares fundamentales que brindan las metodologías ágiles en los tiempos de respuesta que se pueden brindar cuando se debe dar atención a un incidente de seguridad en TI: el análisis exhaustivo de amenazas cibernéticas y capacidad de respuesta en tiempo real.

La detección temprana de amenazas es fundamental, pero no es suficiente, la capacidad de responder de manera rápida y efectiva es igualmente crucial para minimizar el impacto de un ataque cibernético. La respuesta en tiempo real se refiere a la habilidad de una organización para identificar, analizar y neutralizar una amenaza en el momento en que ocurre, o en el menor tiempo posible.

La importancia tanto de la detección temprana como de la respuesta rápida se basa en los siguientes factores:

- Minimizar el impacto
- Preservar la continuidad del negocio
- Fortalecer la resiliencia

Algunas de las herramientas que se utilizan para la respuesta en tiempo real son las siguientes:

- Sistemas de detección y prevención de intrusiones (IPS/IDS)
- Plataformas de seguridad de endpoints (EDR)
- Orquestación y automatización de la seguridad (SOAR)
- Análisis de comportamiento de usuarios y entidades (UEBA)

La integración del análisis de amenazas y la respuesta en tiempo real crea un ciclo de retroalimentación continuo que mejora la seguridad de la organización a lo largo del tiempo. La información obtenida durante la respuesta a incidentes se utiliza para refinar el análisis de amenazas, lo que a su vez mejora la capacidad de la organización para detectar y responder a futuros ataques.

Herramientas ágiles

Las principales metodologías ágiles aplicadas en ciberseguridad son las siguientes:

- Scrum: es una metodología ágil que se enfoca en el trabajo en equipo y la colaboración, el equipo de desarrollo trabaja en ciclos cortos de desarrollo, llamados “sprints”, en los que se enfocan en entregar un conjunto de funcionalidades.
- Kanban: es una metodología ágil que se enfoca en la visualización del trabajo en progreso y la limitación de trabajo en curso. En Kanban, las tareas se representan en tarjetas, que se mueven por un tablero visual, lo que permite al equipo ver de un vistazo el progreso del trabajo.
- XP (Extreme Programming): es una metodología ágil que se enfoca en la calidad del software y la mejora continua del proceso de desarrollo XP, se basa en

prácticas como la programación en parejas, la integración continua, las pruebas automatizadas y el diseño simple.

- DevOps: es la unión de personas, procesos y tecnología para ofrecer valor a los clientes de forma constante, permite que los roles que antes estaban aislados se coordinen y colaboren para producir productos mejores y más confiables.

10. Equipos de trabajo en ciberseguridad

A continuación, se describirán varios de los equipos que se pueden conformar en la atención de incidentes de Ciberseguridad.

Red Team (Equipo Rojo)

Un Red Team se define como un equipo de expertos en Ciberseguridad, esto es, un equipo formado por profesionales de la seguridad informática que actúan como amenazas que intentan superar controles de Ciberseguridad. (TheBridge, 2023)

Lo suelen integrar hackers éticos independientes que evalúan la seguridad del sistema de una empresa de un modo completamente objetivo.

Qué hace un Red Team:

Un Red Team pasa la mayor parte del tiempo planeando un ataque, mucho más que poniéndolo en marcha, despliegan una serie de métodos para lograr el acceso a una red. Antes de poner en marcha una prueba de penetración, hacen uso de rastreadores de paquetes y usan analistas de protocolos que exploran la red y recopilan todos los datos e información posible sobre el sistema.

Cuando el Red Team tiene una idea completa de la situación del sistema, se pone en marcha un plan de acción diseñado para atacar y poner a prueba todas esas vulnerabilidades de las que se han percatado a la hora de recoger la información.

Cómo actúa un Red Team:

Un Red Team pone en marcha ataques que son habituales por parte de los ciberdelincuentes, los hackers reales y los que pueden hacer daño, para ello utilizan las siguientes herramientas:

- Pruebas de penetración
- Ingeniería social
- Phishing
- Clonación de tarjetas de seguridad

Blue Team (Equipo azul)

Son equipos multidisciplinarios compuestos por expertos en ciberseguridad especializados en analizar el comportamiento de los sistemas de una empresa.

Qué hace un Blue Team:

- Reúne datos para documentarse sobre todo aquello que hay que proteger, y efectúa una evaluación de riesgos.
- Refuerza el acceso al sistema de diversas formas, por ejemplo, con políticas más estrictas en materia de seguridad y ejerciendo una función didáctica con los trabajadores de la organización para que entiendan y se ajusten a los procedimientos de seguridad.

- Establece protocolos de vigilancia como blue team, que puedan registrar la información relativa al acceso a los sistemas e ir comprobando si se produce algún tipo de actividad inusual.
- Efectúa comprobaciones periódicas del sistema, como auditorías del sistema de nombres de dominio DNS, de la vulnerabilidad de la red interna o externa, etc.
- Realiza evaluaciones de riesgo identificando las amenazas contra cada activo y las debilidades que pueden explotar.

Procedimientos de un Blue Team en Ciberseguridad:

Algunas de las técnicas de actuación que pone en marcha un Blue Team destacan las siguientes:

- Realizar auditorías del DNS para prevenir ataques de phishing, evitar problemas de DNS caducados, etc.
- Efectuar análisis de la huella digital teniendo la capacidad de rastrear la actividad de los usuarios e identificar las firmas conocidas que puedan alertar de una violación de la seguridad.
- El blue team permite instalar el software de seguridad de puntos finales en dispositivos externos.
- Se encarga de asegurar que los controles de acceso al cortafuegos tengan la configuración correcta y mantener el software antivirus actualizado.
- Desplegar software IDS e IPS para controlar la seguridad de detección y prevención.
- Estos equipos de ciberseguridad permiten aplicar soluciones SIEM para registrar y absorber la actividad de la red.

- Efectuar un análisis de los registros y la memoria para recabar datos sobre algún tipo de actividad inusual en el sistema e identificar y localizar un ataque informático.
- Segregar las redes y asegurarse de que su configuración es la correcta.
- Implementar un software de exploración de vulnerabilidades.
- Estos equipos de ciberseguridad permiten implementar un software antivirus o antimalware.

Purple Team (Equipo púrpura)

El equipo púrpura no es solo aquel que ejerce funciones defensivas y ofensivas (equipos rojo y azul), sino que también es el que facilita la comunicación y optimiza el rendimiento entre ellos.

Es un equipo que se encarga de simular ataques y, a la vez, monitorear y fortalecer el esquema de seguridad de la organización. En algunas ocasiones puede tratarse de un equipo pequeño de seguridad, conformado por pocos integrantes que ejercen los papeles tanto del Red Team como del Blue Team, aunque esto no implica que la función del Purple Team se reduzca solo a estos casos.

En los equipos de seguridad más completos, su función es maximizar la efectividad de los equipos rojo y azul, a través del desarrollo de objetivos comunes, así como facilitar la comunicación entre ambos grupos.

En síntesis, el equipo púrpura ayuda a optimizar el rendimiento de los equipos rojo y azul y de esta forma la seguridad de la organización.

Interacción entre equipos

La interacción entre los diferentes equipos de ciberseguridad es muy importante en una organización, tanto el Red Team, como el Blue Team, así como el Purple Team. El objetivo de tener equipos adversarios es mejorar aún más la Seguridad de una organización. Sin embargo, este enfoque es imperfecto porque, por lo general, descuida errores fundamentales en la forma en que estos equipos cooperan entre sí.

La relación tradicional de adversarios no funciona, enfrentar al Red Team contra el Blue Team es cosa del pasado, por el contrario, ahora se busca entrelazar las dos unidades para crear una relación simbiótica que permita obtener resultados mucho mejores para ambos equipos. Esto se conoce como el Purple Team, aunado a esto la automatización desempeña un valioso papel en los entornos de Seguridad actuales, pues los resultados suelen ser mejores cuando los equipos red y blue logran más con menos.

En el panorama actual de la Seguridad, la relación de adversarios tradicional no funciona, es mucho mejor combinar las dos unidades para crear un "Purple Team" que mejore la cooperación y permita lograr mejores resultados.

La colaboración es la clave, algunas de las acciones que se deben tomar son las siguientes:

- Mantener un debate continuo y sencillo sobre el progreso de la interacción.
- Utilizar la plataforma para dirigirse directamente a las personas sobre un tema de modo que cada miembro del equipo pueda interactuar de forma rápida y eficaz sin tener que rebuscar correos electrónicos ni recordar llamadas telefónicas.
- Utilizar Microsoft Teams, Slack y otras plataformas de comunicación para invitar a terceros a interactuar directamente con cada uno de los equipos.

Beneficios del uso de equipos de trabajo en ciberseguridad

Para entender y tener claridad de los beneficios que el uso de equipos de trabajo en ciberseguridad brinda a una organización es importante tener claros algunos conceptos.

Resiliencia cibernética:

Es la capacidad de una organización para prevenir, resistir y recuperarse de incidentes de ciberseguridad. Es un concepto que aúna la continuidad del negocio, la seguridad de los sistemas de información y la resiliencia organizacional.

Un nivel medido de competencia y resiliencia en materia de seguridad de la información influye en la capacidad de una organización para continuar sus operaciones comerciales con un tiempo de inactividad mínimo o nulo. (IBM, 2023)

Existe además el concepto de resiliencia cibernética efectiva, que debe ser una estrategia empresarial basada en el riesgo, un enfoque de colaboración impulsado desde los ejecutivos hasta todos los miembros de la organización, los socios, los participantes de la cadena de suministro y los clientes. Debe gestionar de forma proactiva los riesgos, las amenazas, las vulnerabilidades y los efectos en la información crítica y los activos de apoyo.

Optimización de la respuesta a incidentes:

De acuerdo con IBM una respuesta a incidentes “se refiere a los procesos de tecnologías de una organización para detectar y responder a amenazas cibernéticas, violaciones de seguridad o ciberataques. Un plan formal de respuesta a incidentes permite a los equipos de ciberseguridad limitar o prevenir daños. (IBM, 2023)

Su objetivo es prevenir los ataques cibernéticos antes de que ocurran y minimizar el costo y la interrupción del negocio resultantes de cualquier ataque cibernético que ocurra. Es la parte

técnica de la gestión de incidentes, que también incluye la gestión ejecutiva, de RR.HH. y legal de un incidente grave.

Un plan eficaz de respuesta a incidentes puede ayudar a los equipos de respuesta a incidentes cibernéticos a detectar y contener amenazas cibernéticas, restaurar los sistemas afectados y reducir la pérdida de ingresos, las multas regulatorias y otros costos.

Generalmente un plan de respuesta a incidentes incluye:

- Un manual de estrategias de respuesta a incidentes
- Las soluciones de seguridad instaladas en toda la empresa
- Un plan de continuidad del negocio que describa los procedimientos para restaurar los sistemas y datos críticos lo más rápido posible en caso de una interrupción.
- Una metodología de respuesta a incidentes
- Un plan de comunicación
- Instrucciones para recopilar y documentar información

Detección temprana de amenazas

La detección de amenazas es un proceso de ciberseguridad para identificar ciberamenazas en los recursos digitales de una organización y tomar medidas para mitigarlas lo antes posible. Para anticiparse a los crecientes ataques de ciberseguridad, las organizaciones usan el modelado de amenazas para definir los requisitos de seguridad, identificar vulnerabilidades y riesgos, y priorizar la corrección. La primera acción en este punto es crear un Centro de Operaciones de Seguridad (SOC) que es una función centralizada o un equipo responsable de mejorar la posición de ciberseguridad de una organización y de evitar, detectar y responder ante las amenazas.

Con los escenarios hipotéticos, el SOC intenta entrar en la mente de los ciberdelincuentes para que puedan mejorar la capacidad de la organización para evitar o mitigar incidentes de seguridad.

Una vez identificada una ciberamenaza, la respuesta ante amenazas incluye las acciones que realiza el SOC para contenerla y eliminarla, recuperarla y reducir las posibilidades de que vuelva a producirse un ataque similar.

11.Estándares internacionales en ciberseguridad

A continuación, se van a detallar algunos de los estándares internacionales más importantes en cuanto a ciberseguridad que existen actualmente.

ISO/IEC 27001

Es la norma más conocida del mundo para sistemas de gestión de la seguridad de la información (SGSI). Esta norma define los requisitos que debe cumplir un SGSI.

Esta norma proporciona a las empresas de cualquier tamaño y de todos los sectores u orientaciones para establecer, implantar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información.

La conformidad con la norma ISO/IEC 27001 implica que una organización o empresa ha implantado un sistema para gestionar los riesgos relacionados con la seguridad de los datos que posee o maneja, y que este sistema respeta todas las buenas prácticas y principios contemplados en esta Norma Internacional. (ISO, 2022)

Por qué es importante la norma ISO/IEC 27001

Esta Norma ayuda a las organizaciones a ser conscientes de dichos riesgos y a identificar y abordar los puntos débiles de forma proactiva. Promueve además un enfoque integral de la seguridad de la información, que abarca a las personas, las políticas y la tecnología. Un sistema

de gestión de la seguridad de la información implantado conforme a esta norma es una herramienta clave para la gestión de riesgos, la resiliencia cibernética y la excelencia operativa.

Beneficios de la Norma ISO/IEC 27001

Estos son los beneficios que brinda la implementación de la norma ISO/IEC 27001 en una organización:

- Resistencia a los ciberataques
- Preparación ante nuevas amenazas
- Integridad, confidencialidad y disponibilidad de la información
- Seguridad en todos los soportes
- Protección en toda la empresa
- Ahorro de costos

NIST Cybersecurity framework

Es un enfoque ampliamente utilizado, basado en estándares, pautas y prácticas existentes para ayudar a las organizaciones a gestionar y reducir mejor el riesgo de ciberseguridad.

Proporciona a las pequeñas y medianas empresas (PYMES), específicamente a aquellas que tienen planes de ciberseguridad modestos o nulos, consideraciones para poner en marcha su estrategia de gestión de riesgos de ciberseguridad utilizando el NIST Cybersecurity Framework 2.0. (NIST, 2024)

Este marco consta de estándares, pautas, y mejores prácticas que ayudan a las organizaciones a mejorar su gestión de riesgos de ciberseguridad. El diseño del CSF del NIST tiene una flexibilidad que le permite integrarse con los procesos de seguridad existentes dentro de cualquier organización, en cualquier industria. Proporciona un excelente punto de partida para

implementar la seguridad de la información y la gestión de riesgos de ciberseguridad en prácticamente cualquier organización del sector privado en los Estados Unidos.

Niveles de implementación del marco NIST

- Nivel 1- Parcial
- Nivel 2- Riesgo informado
- Nivel 3- Repetible
- Nivel 4 – Adaptable

Las actividades clave del CSF incluyen:

- Garantizar que los procesos de planificación de respuesta se ejecuten durante y después de un incidente.
- Gestión de las comunicaciones con las partes interesadas internas y externas durante y después de un evento
- Analizar el incidente para garantizar una respuesta eficaz y apoyar las actividades de recuperación, incluido el análisis forense y la determinación del impacto de los incidentes.
- Realizar actividades de mitigación para prevenir la expansión de un evento y resolver el incidente.
- Implementar mejoras incorporando lecciones aprendidas de actividades de detección/respuesta actuales y anteriores.

Estas actividades permiten a las organizaciones responder de manera rápida y eficaz a los incidentes de ciberseguridad, minimizando los daños y facilitando una recuperación rápida. La función Responder garantiza que una organización pueda gestionar y recuperarse de los incidentes manteniendo al mismo tiempo la continuidad del negocio.

Los principales beneficios de implementar el NIST CSF 2.0 son los siguientes:

- Gestión integral de riesgos
- Flexibilidad y escalabilidad
- Cumplimiento normativo
- Resiliencia cibernética mejorada
- Reconocimiento de la industria
- Mejores informes a la junta directiva

OWASP

El proyecto abierto de seguridad de aplicaciones web (OWASP), es una organización internacional sin ánimo de lucro dedicada a la seguridad de aplicaciones web. Uno de sus principios fundamentales es que todos sus materiales están disponibles de forma gratuita y son fácilmente accesibles en su sitio web, lo cual posibilita que cualquiera pueda mejorar la seguridad de su propia aplicación web. (Cloudfare, 2023)

El objetivo de la metodología OWASP se sustancia en dos objetivos principales. Por un lado, advertir a los desarrolladores de los peligros que orbitan en Internet y de los errores más frecuentes que se cometen a la hora de diseñar y crear software y hardware. Por otro, ofrecer herramientas de acceso libre con las que analizar la seguridad de las soluciones y dispositivos que lanzan al mercado.

OWASP adopta un enfoque multifacético para la seguridad de aplicaciones web y móviles, que abarca varios aspectos clave:

- OWAS Top 10: es un informe ampliamente reconocido que describe los diez riesgos de seguridad de aplicaciones web más críticos.

- OWAS Application Security Estándar de verificación (ASVS): el sistema Application Security Verification Standard es una guía completa para profesionales de seguridad, desarrolladores y proveedores de aplicaciones que describe las mejores prácticas para el desarrollo seguro de aplicaciones, establece una base para las medidas de seguridad de las aplicaciones, garantizando que estas no solo se desarrollen teniendo en cuenta la funcionalidad, sino que también sean seguras contra una gran cantidad de amenazas potenciales.
- OWASP Seguridad de aplicaciones móviles Guía de prueba (MASTG): proporciona una metodología integral para probar la seguridad de aplicaciones móviles, MASTG ofrece orientación adaptada específicamente a plataformas móviles, reconociendo sus desafíos y consideraciones de seguridad únicos.

Los principios fundamentales de OWASP enfocados hacia la seguridad de las aplicaciones son los siguientes:

- Principios de diseño seguro: OWASP enfatiza la importancia de integrar consideraciones de seguridad a lo largo de todo el ciclo de vida de desarrollo de software (SDLC). Esto incluye prácticas de codificación segura, modelado de amenazas y revisiones de arquitectura en las primeras etapas de la fase de desarrollo.
- Metodología de calificación de riesgo: OWASP alienta a las organizaciones a adoptar un enfoque basado en riesgos para la seguridad de las aplicaciones, esto implica identificar aplicaciones críticas, evaluar posibles amenazas a la seguridad

y priorizar las vulnerabilidades en función de su gravedad y probabilidad de explotación.

Limitaciones en la implementación de OWASP

- Restricciones de recursos y presupuesto
- Complejidad y desafíos técnicos
- Integración con procesos existentes
- Alcance y escalabilidad
- Capacitación y Concienciación

Beneficios de adoptar el enfoque OWASP

- Postura de seguridad mejorada
- Prácticas de seguridad estandarizadas
- Rentabilidad
- Cumplimiento de la normativa
- Educación y concienciación mejoradas para los desarrolladores
- Apoyo y recursos comunitarios
- Flexibilidad y adaptabilidad

CIS Controls

Los controles de seguridad del CIS son un conjunto de prácticas recomendadas prescriptivas, priorizadas y simplificadas que puede utilizar para fortalecer su postura en materia de ciberseguridad. En la actualidad, miles de profesionales de la ciberseguridad de todo el mundo utilizan los controles del CIS o contribuyen a su desarrollo a través de un proceso de consenso comunitario. (cisecurity, 2024)

Con los controles CIS, se pueden obtener los siguientes logros:

- Simplificar el enfoque de protección contra amenazas
- Cumplir con las regulaciones de la industria
- Lograr una higiene cibernética esencial
- Traducir la información a la acción
- Atender a la ley

Los controles CIS se actualizan regularmente para adaptarse a las amenazas en constante evolución, garantizando que las organizaciones se mantengan al día con las vulnerabilidades emergentes y las estrategias de mitigación.

A continuación, se describen los 18 controles CIS:

- Inventario y control de activos empresariales: gestionar activamente todos los dispositivos de hardware en la red para que solo los dispositivos autorizados tengan acceso y se detecten y eviten los dispositivos no autorizados y no administrados que intenten obtener acceso.
- Inventario y control de activos de software: gestionar activamente todo el software en la red para que solo se instale y ejecute software autorizado, y para encontrar y prevenir la instalación o ejecución de software no autorizado y no administrado.
- Protección de datos: establecer y mantener un inventario de los datos que deben protegerse, clasificarlos según su nivel de sensibilidad y asegurarse de que estén protegidos adecuadamente.
- Configuración segura de activos y software empresariales: establecer, implementar y gestionar activamente la configuración de la seguridad de los activos empresariales utilizando un riguroso proceso de gestión de

configuraciones y control de cambios para prevenir que los atacantes aprovechen servicios y configuraciones vulnerables.

- Gestión de cuentas: controlar el acceso a sistemas y aplicaciones basado en el principio de privilegio mínimo; limitar el acceso innecesario a datos sensibles; restringir el acceso a sistemas críticos; asegurarse de que las cuentas se asignen solo a usuarios autorizados; asegurarse de que las cuentas se desactiven cuando ya no sean necesarias o cuando un empleado abandone la organización.
- Gestión de control de acceso: asegurarse de que solo los usuarios autorizados tengan acceso a sistemas y aplicaciones en función de sus funciones laborales asignadas; garantizar que los usuarios tengan solo los privilegios necesarios para realizar sus funciones laborales; monitorear la actividad de los usuarios en busca de acciones no autorizadas.
- Gestión continua de vulnerabilidades: adquirir, evaluar y actuar de manera continua sobre nueva información para identificar vulnerabilidades, remediarlas de manera oportuna y minimizar la ventana de oportunidad para los atacantes.
- Gestión de registros de auditoría: recopilar registros de auditoría de todos los sistemas y componentes de redes; almacenar los registros de forma segura; revisar regularmente los registros en busca de signos de actividad sospechosa; retener los registros durante un período de tiempo adecuado.
- Protección de correo electrónico y navegador web: proteger los sistemas de correo electrónico contra ataques de phishing mediante la implementación de controles técnicos como el filtrado de correo electrónico; proteger los navegadores web

contra código malicioso mediante la implementación de controles técnicos como el filtrado web.

- Defensas contra malware: protegerse contra el malware mediante la implementación de controles técnicos como el software antivirus; establecer políticas para manejar incidentes de malware.
- Recuperación de datos: asegurarse de que los datos se puedan recuperar en caso de un incidente de pérdida de datos mediante la implementación de controles técnicos como las copias de seguridad; probar regularmente las copias de seguridad.
- Gestión de infraestructura de red: gestionar dispositivos de infraestructura de red como enrutadores, conmutadores, firewalls, etc., utilizando procesos rigurosos de gestión de configuración y control de cambios para evitar que los atacantes aprovechen servicios y configuraciones vulnerables.
- Monitoreo y defensa de la red: monitorear las redes en busca de signos de actividad sospechosa; responder de manera rápida a los incidentes; establecer políticas para manejar los incidentes.
- Concientización y capacitación en seguridad: capacitar a los empleados sobre cómo reconocer ataques de phishing; establecer políticas para informar actividades sospechosas.
- Gestión de proveedores de servicios: asegurarse de que los proveedores de servicios de terceros sean responsables de cumplir con los requisitos de seguridad; establecer políticas para manejar incidentes que involucren a proveedores de servicios de terceros.

- Seguridad de software de aplicación: asegurarse de que el software de aplicaciones se desarrolle de manera segura siguiendo prácticas de codificación segura; realizar pruebas periódicas de las aplicaciones para identificar vulnerabilidades de seguridad.
- Gestión de respuesta a incidentes: establecer un plan de respuesta a incidentes que incluya procedimientos para detectar incidentes, responder a ellos, informar a las partes apropiadas, recuperarse de los incidentes y realizar revisiones posteriores a los incidentes.
- Pruebas de penetración: realizar ejercicios regulares de pruebas de penetración para identificar vulnerabilidades antes que los atacantes; realizar ejercicios de equipo rojo para probar la efectividad de los controles de seguridad; realizar ejercicios de simulación de respuesta a incidentes para probar la efectividad de los planes de respuesta a incidentes.

Estándares de seguridad para la protección de empresas aseguradoras

En el mercado actual, las organizaciones buscan demostrar confianza a sus clientes y compromiso con la seguridad de la información que manejan. Para estos fines, el hecho de poseer una certificación de algún estándar o norma ISO referente a Seguridad representa una ventana competitiva, pues esto es consecuencia de una correcta gestión de los requisitos de seguridad en los procesos de tratamiento de la información.

La implementación de medidas eficaces de ciberseguridad no es algo sencillo ya que, debido a la gran cantidad de equipos y tecnologías utilizadas, los ciberdelincuentes siempre encuentran nuevas opciones de llevar a cabo sus ataques.

Con el fin de protegerse contra estas amenazas, existen los estándares y normas ISO que se relacionan con la ciberseguridad y seguridad de la información, estas normas son estándares desarrollados y publicados por la Organización Internacional de Normalización (ISO).

Específicamente en el sector de los seguros las empresas enfrentan desafíos de ciberseguridad cada vez mayores, en el año 2021 por ejemplo, algunas de las principales empresas del sector sufrieron ciberincursiones.

Estos incidentes han puesto de relieve la creciente amenaza de los ciberdelincuentes que intentan explotar las lagunas en las redes y sistemas de seguros.

Los ciberataques a compañías de seguros tienen múltiples repercusiones, estas empresas recopilan, procesan y almacenan una amplia gama de datos personales y confidenciales de los clientes, incluidos detalles financieros, médicos y legales, esto los convierte en un objetivo atractivo para los ataques cibernéticos.

De acuerdo con la página safecore (safecore, 2023) se estima que los ingresos relacionados con la ciberseguridad en la industria de seguros crecerán a una tasa anual compuesta de más del 10 % alcanzando aproximadamente 10,6 millones de dólares en el año 2025.

En este contexto, las compañías de seguros están llamadas a gestionar con prudencia la cuestión de la ciberseguridad, para evitar daños a su reputación y a sus relaciones con los clientes.

Evolución tecnológica en el sector asegurador:

La evolución tecnológica en este sector está generando importantes transformaciones y oportunidades para las compañías de seguros. Estos cambios afectan a muchos aspectos de la industria, desde la evaluación de riesgos hasta la gestión de reclamaciones y la interacción con el cliente. Algunas de las principales tendencias tecnológicas en la industria de seguros incluyen:

- Big data y analítica avanzada
- Inteligencia artificial (IA) y aprendizaje automático
- Internet de las cosas (IoT) y telemática

La innovación en los servicios de seguros se ha vuelto cada vez más importante en la actual era digital. Las tecnologías digitales, como la inteligencia artificial, el análisis de datos y la cadena de bloques, pueden ayudar a crear productos de seguros personalizados y mejorar la eficiencia de los procesos comerciales.

Vulnerabilidades existentes en el sector:

Estas son algunas de las vulnerabilidades claves en la industria:

- La seguridad cibernética: principalmente se enfrentan al riesgo de filtraciones de datos, ataques de phishing y ransomware. (KPMG, 2024)
- Cambios regulatorios: normalmente las empresas están sujetas a estrictas regulaciones gubernamentales y deben cumplir con leyes de protección de datos entre otras cosas. (KPMG, 2024)
- Adicción a la tecnología: la adopción de tecnologías avanzadas puede conducir a una mayor dependencia de los proveedores de servicios de tecnología y sistemas complejos. (KPMG, 2024)
- Integración y compatibilidad del sistema: la integración de sistemas y tecnologías puede crear desafíos de interoperabilidad y compatibilidad. (KPMG, 2024)

- Confidencialidad y privacidad de los datos: este es un tema crítico en la industria de seguros, pues las compañías recopilan, procesan y almacenan grandes cantidades de datos personales y confidenciales sobre sus clientes. (KPMG, 2024)

Directrices de ciberseguridad en el sector asegurador

Las directrices de ciberseguridad en el sector asegurador son básicas para proteger a las empresas y a sus clientes de los riesgos de ciberseguridad, algunas de las principales son las siguientes:

- Formación y sensibilización: se debe promover la concienciación y la formación sobre riesgos cibernéticos entre sus empleados, clientes y socios. (safecore, 2023)
- Protección de datos y privacidad: deben contar con políticas y procedimientos estrictos para garantizar la protección de los datos confidenciales de los clientes y el cumplimiento de leyes de privacidad y protección de datos. (safecore, 2023)
- Seguridad de la infraestructura de TI: la red corporativa debe ser monitoreada constantemente para identificar cualquier ciberataque o anomalía en la gestión de datos. (safecore, 2023)
- Gestión de parches y actualizaciones de software: es esencial mantener actualizados los sistemas operativos, el software y las aplicaciones para proteger la infraestructura de TI de las vulnerabilidades conocidas. (safecore, 2023)
- Gestión de acceso y autenticación: las compañías de seguros deben implementar políticas de administración de acceso para garantizar que solo los usuarios autorizados tengan acceso a los sistemas y la información confidencial. (safecore, 2023)

Retos de ciberseguridad en el sector de seguros

Los desafíos principales en materia de ciberseguridad que tienen las compañías de seguros son:

- Digitalización e innovación tecnológica: adaptarse a las nuevas tecnologías y la digitalización e integrarlas a los procesos comerciales es clave para mantenerse competitivo. (safecore, 2023)
- Cambio climático y desastres naturales: la creciente frecuencia y severidad de los desastres naturales relacionados con el cambio climático está ejerciendo presión sobre la industria de seguros. (safecore, 2023)
- Complejidad tecnológica: se manejan grandes cantidades de datos y utilizan muchas tecnologías diferentes, lo que hace que proteger la infraestructura de TI sea una tarea compleja. (safecore, 2023)
- Aumento de amenazas cibernéticas: las compañías se han vuelto cada vez más vulnerables a los ciberataques, que pueden poner en riesgo la reputación de la compañía. (safecore, 2023)

12. Gestión de riesgos en ciberseguridad

IBM define la gestión de riesgos en ciberseguridad de la siguiente manera: “es el proceso de identificar, priorizar, gestionar y monitorizar los riesgos de los sistemas de información”. (IBM, 2022)

La gestión de ciberriesgos se ha convertido en una parte fundamental de los esfuerzos de gestión de riesgos empresariales más amplios. Empresas de todos los sectores dependen de la tecnología de la información para llevar a cabo funciones de negocio claves en la actualidad, esto

las expone a los ciberdelincuentes, los errores de los empleados (error humano), desastres naturales y otras amenazas de ciberseguridad.

Si bien estos riesgos no se pueden eliminar, los programas de gestión de ciberriesgos pueden ayudar a reducir el impacto y la probabilidad de amenazas. Las empresas utilizan este proceso de gestión de ciberriesgos para identificar sus amenazas más cruciales y seleccionar medidas de seguridad de TI adecuadas para proteger los sistemas de información de los ciberataques y otras amenazas digitales.

Los mismos tipos de ciberataques pueden tener diferentes consecuencias según la compañía, de acuerdo con la web de IBM, en el sector sanitario las vulneraciones de datos cuestan en promedio 10,10 millones de dólares, mientras que las filtraciones en el sector hotelero cuestan 2,9 millones de dólares, de acuerdo con el "Cost of Data Breach" de IBM. (IBM, 2023)

Los pasos básicos que se siguen en los diferentes métodos de gestión de riesgos son los siguientes:

- Marco de riesgo: es el acto de definir el contexto en el que se toman las decisiones de riesgo, cuando se enmarca el riesgo desde el principio, las empresas pueden alinear sus estrategias de gestión de riesgos con sus estrategias empresariales generales.
- Evaluación de riesgos: las evaluaciones de riesgos se usan para identificar amenazas y vulnerabilidades, estimar sus potenciales y priorizar los riesgos más cruciales.
- Respuesta al riesgo: con los resultados de la evaluación de riesgos la empresa puede determinar cómo responderá a los riesgos potenciales, los poco probables o

de bajo impacto, pueden simplemente aceptarse, pues invertir en medidas de seguridad puede ser más caro que el propio riesgo.

- Supervisión: la organización supervisa sus nuevos controles de seguridad para verificar que funcionan según lo previsto y cumplen con los requisitos normativos pendientes.

Importancia de la gestión del riesgo cibernético

El panorama general de las amenazas evoluciona constantemente, cada mes, se añaden aproximadamente 2000 vulnerabilidades en la base de datos del NIST, se detectan miles de nuevas variantes de malware mensualmente y ese es solo un tipo de ciberamenaza.

Las iniciativas de gestión de ciberriesgos pueden ayudar a las organizaciones a cumplir con las leyes de Protección de Datos, y las leyes propias de cada país. Durante el proceso de la implementación de esta gestión de riesgos, las empresas consideran estos estándares al diseñar sus programas de seguridad.

Análisis de riesgos

Existen varios métodos para evaluar el riesgo de ciberataques, a continuación, se van a describir dos de ellos:

FMEA (Failure mode and effects analysis)

Es un método estructurado que tiene como objetivo identificar fallas potenciales y sus resultados correspondientes. Es un enfoque considerado de abajo hacia arriba; el análisis comienza con datos específicos que se acumulan para formar un plan de acción más general. En este caso, cada componente del sistema observado se examina minuciosamente en busca de posibles causas de avería.

El desarrollo de un proceso FMEA equipa a las organizaciones con una estrategia para identificar posibles averías incluso antes de que ocurran. Este proceso puede optimizar los esfuerzos de los equipos de mantenimiento para aumentar la confiabilidad de manera eficiente.

FMEA funciona recopilando la mayor cantidad de información posible del piso de producción. Los equipos de mantenimiento y confiabilidad, al estar más cerca de los equipos y procesos, son activos valiosos para proporcionar una colección de ideas sobre cómo pueden ocurrir fallas. Luego se evalúan los efectos de cada falla potencial. Finalmente, la gravedad de cada uno de los efectos se califica y evalúa para formar una escala ponderada.

Debido a la asignación de pesos que realiza FMEA, se convierte en un criterio de decisión objetivo con el que se pueden alinear las funciones de la organización. Un número de prioridad de riesgo (RPN) se refiere al valor de riesgo al que asciende cada resultado, este RPN se convierte en la base de si los equipos deben o no tomar medidas para abordar una posible falla, es importante que los equipos de mayor relevancia tengan el mismo nivel de comprensión de la RPN y sus acciones correspondientes.

Los efectos en FMEA son los siguientes:

- Efecto local
- Siguiente efecto de nivel superior
- Efecto final

Los componentes de un proceso FMEA son los siguientes:

- Probabilidad de falla
- Detectabilidad
- Gravedad

La introducción de un proceso FMEA en una organización debe contar con la aprobación de la alta gerencia, sin embargo, siempre se va a requerir una acción colectiva que involucre a toda la organización.

Los pasos necesarios para iniciar el proceso se describen a continuación:

- Identificar el componente, equipo, sistema o proceso a analizar
- Asigne un equipo y un líder de equipo que iniciaría el proceso.
- Describir lo que se está analizando
- Identificar posibles modos de falla
- Identificar los efectos relacionados con los modos de falla
- Establecer los criterios para evaluar el riesgo de cada modo de falla y sus efectos.
- Diseñar un método de priorización basado en el Número de Prioridad de Riesgo calculado a partir de componentes previamente evaluados.
- Tomar las acciones necesarias para eliminar o reducir los riesgos identificados
- Medir el éxito de la reducción de riesgos luego de implementar las acciones establecidas.

CVA (Critical vulnerability assesment)

Una evaluación crítica de vulnerabilidades es un proceso que se utiliza para identificar y asignar niveles de gravedad a la mayor cantidad posible de defectos de seguridad en un período de tiempo determinado. Este proceso puede implicar técnicas automatizadas y manuales con distintos grados de rigor y un énfasis en la cobertura integral. Mediante un enfoque basado en el riesgo, las evaluaciones de vulnerabilidades pueden apuntar a diferentes capas de tecnología, siendo las más comunes las evaluaciones de la capa de host, red y aplicación.

Una evaluación de este tipo tiene tres objetivos principales:

- Identificar vulnerabilidades que van desde fallas críticas de diseño hasta simples configuraciones erróneas.
- Documentar las vulnerabilidades para que los desarrolladores pueden identificar y reproducir los hallazgos fácilmente.
- Crear una guía para ayudar a los desarrolladores a remediar las vulnerabilidades identificadas.

Estas pruebas pueden adoptar distintas formas, uno de estos métodos es la prueba de seguridad de aplicaciones dinámicas (DAST), también existe la prueba llamada de Seguridad de aplicaciones estáticas (SAST), este es al análisis del código fuente o el código objeto de una aplicación para identificar vulnerabilidades sin ejecutar el programa.

Evaluación de impacto y probabilidad

El identificador EPSS (Exploit Prediction Scoring System) cuantifica la probabilidad de que una determinada vulnerabilidad sea explotada en los próximos 30 días.

De acuerdo con el Common Vulnerabilities and Exposures (CVE), que es un diccionario que recopila, sistematiza y estandariza la forma de denominar a todas las vulnerabilidades, incluye actualmente más de 200 mil. El 10 % de ellas son consideradas críticas por el CVSS (Common Vulnerability Scoring System), además, el número de vulnerabilidades aumenta año con año, por ejemplo, en el año 2022 se batió el récord histórico, tras descubrir 25.227 vulnerabilidades en esos 12 meses.

Por este motivo, existen herramientas como el EPSS, basada en datos que sirve para estimar la probabilidad de que una vulnerabilidad sea explotada en los siguientes 30 días.

EPSS emplea datos permanentemente actualizados sobre amenazas y exploits para otorgar una puntuación de probabilidad entre 0 y 1, siendo un 100 % de probabilidad de

explotación. De esta manera, EPSS ayuda a los profesionales de ciberseguridad y a las compañías de todo el mundo a conocer cuán probable es que una vulnerabilidad sea explotada en el corto plazo y puedan tomar medidas para mitigarlas antes de que se produzcan incidentes de seguridad.

Utilizando el machine learning, esta herramienta puede detectar patrones en los datos con los que se alimenta el modelo del EPSS y realizar predicciones que permiten aventurar la probabilidad de explotación de cada una de las vulnerabilidades publicadas en CVE.

La IA y los datos se sitúan como los elementos capitales del sistema de puntaje, estos datos se combinan con dos tipologías de fuentes: información sobre las amenazas y datos de explotación de vulnerabilidades.

Algunas de las estrategias para priorizar la remediación de vulnerabilidades son las siguientes:

- Eficiencia en la gestión de los recursos
- Cobertura de las actividades de remediación
- EPSS v3

De esta forma, la gestión de vulnerabilidades se convierte en una actividad esencial de la estrategia de seguridad defensiva de una empresa, lo cual sirve para evaluar el estado global de seguridad a partir de las siguientes actividades:

- Gestión de los riesgos de seguridad
- Monitoreo permanente de la infraestructura de TI
- Elaboración de un plan de detección y remediación de vulnerabilidades
- Optimizar la capacidad de detección de nuevas vulnerabilidades
- Diseño de estrategias de mitigación de debilidades

- Supervisión de la subsanación de vulnerabilidades
- Cumplimiento de los requerimientos normativos en vigor

Planes de mitigación

Los atacantes están encontrando cada vez formas más sofisticadas de tener acceso, inspeccionar y manipular sistemas de control de infraestructura critica de manera ilícita, y, como contrapartida, las prácticas y los productos de seguridad evolucionan constantemente.

La protección de todos los puntos de acceso de red externos e internos es una de las cosas más importantes que puede hacer para aumentar la seguridad cibernética de los sistemas. Es importante contar con un inventario de las vías de comunicaciones y los puntos de acceso que son necesarios y luego deshabilitar todos los puertos de comunicación sin utilizar. Debe tenerse en cuenta también los puertos USB que son potenciales puntos de vulnerabilidad para los virus y el malware que se propagan mediante unidades de este tipo.

Existen varios tipos de estrategias que se pueden utilizar para mitigar los riesgos de ciberseguridad, se mencionan 6 de estos a continuación:

- Realizar una evaluación de riesgos cibernéticos
- Establecer controles de acceso a la red
- Monitorizar continuamente la infraestructura de TI
- Crear un plan de respuesta a incidentes (IRP)
- Examinar las medidas de seguridad física de su empresa
- Minimizar la superficie de ataque

Las estrategias de mitigación de riesgos en las empresas son herramientas clave para prevenir o reducir los problemas potenciales que pueden afectar el éxito y la supervivencia de

una organización en materia de ciberseguridad. Estas estrategias ayudan a identificar y gestionar los riesgos de una forma proactiva y eficiente, lo que contribuye a aumentar la seguridad y el crecimiento de la empresa.

CAPÍTULO 3: MARCO METODOLÓGICO

En este se presenta la metodología de trabajo adoptada para su desarrollo, detallando los enfoques y estrategias empleados para la recopilación de datos e insumos esenciales. Asimismo, se describen las herramientas y recursos utilizados para asegurar la calidad y pertinencia de la información obtenida, orientada al cumplimiento de los objetivos establecidos.

a. Enfoque de la investigación

De acuerdo con Roberto Hernández Sampieri, existen tres tipos de enfoques en una investigación: cualitativa, cuantitativa y mixta. (Hernández-Sampieri, 2018).

El enfoque de una investigación se define como la naturaleza del estudio y abarca el proceso investigativo en todas sus etapas: desde la definición del tema y el planteamiento del problema de investigación, hasta el desarrollo de la perspectiva teórica, la definición de la estrategia metodológica, y la recolección, análisis e interpretación de los datos. De esta forma, la selección del enfoque de investigación nunca se reduce a un asunto al azar o capricho, sino, a decisiones de quien investiga, en función de la construcción del problema y las metas del estudio. (InvestigaliaCR, 2023)

El enfoque comprende todo el proceso investigativo y las etapas y los elementos que lo conforman, lo cual implica que cada enfoque tenga características particulares respecto a diversos aspectos de la investigación. (InvestigaliaCR, 2023)

Existen algunos aspectos clave para comprender la comparación que existe en los enfoques cualitativos y cuantitativos, entre otros:

- El tipo de realidad que estudia

- Las metas de la investigación
- La lógica del proceso investigativo
- El tipo de datos del estudio.

b. Tipo de enfoque de la investigación

A continuación, se definen los tres tipos de enfoques de investigación:

b1. Investigación cualitativa

La investigación cualitativa es un enfoque esencial en diversas disciplinas académicas y campos profesionales, pues trata de comprender e interpretar los significados, las experiencias y las realidades sociales de las personas en sus entornos naturales. Este tipo de investigación emplea una serie de métodos cualitativos para recopilar y analizar datos no numéricos, como palabras, imágenes y comportamientos y pretende generar percepciones profundas y contextualizadas de los fenómenos objeto de estudio. (atlasti, 2023)

Está diseñada para abordar cuestiones de investigación que se centran en comprender el por qué y el cómo del comportamiento, las experiencias y las interacciones humanas, en lugar de solo el "qué" o el "cuántos" que suelen tratar de responder los métodos cuantitativos. El objetivo principal de este tipo de investigación es obtener una comprensión rica y profunda de las perspectivas, emociones, creencias y motivaciones de las personas en relación con cuestiones, situaciones o fenómenos específicos. (atlasti, 2023)

Algunas de las características principales son:

- Entornos naturalistas
- Enfoque inductivo
- Perspectiva holística
- Subjetividad e interpretación

- Flexibilidad

Este tipo de investigación está regido por varios principios fundamentales que conforman su enfoque, métodos y análisis, estos son:

- Empatía y reflexividad
- Confianza
- Análisis iterativo
- Descripción detallada

Algunos de los tipos más comunes de investigación cualitativa son:

- Investigación narrativa
- Fenomenología
- Teoría fundamentada
- Etnografía
- Estudio de casos

Existen también varios métodos de investigación cualitativa, esto se refiere a técnicas utilizadas para recopilar, analizar e interpretar datos en estudios cualitativos. Estos métodos dan prioridad a la exploración del significado, el contexto y las experiencias individuales, algunos de los métodos más comunes son:

- Entrevistas
- Grupos focales
- Observaciones
- Análisis de documentos
- Métodos visuales

b2. Investigación cuantitativa

Este tipo de investigación tiene como objetivo principal la cuantificación de los datos, esto permite generalizar los datos de una muestra a toda una población de interés y medir la incidencia de diversos puntos de vista y opiniones en una muestra determinada. La investigación cuantitativa se considera especialmente adecuada para comprender en profundidad las razones y motivaciones subyacentes. Proporciona información sobre el entorno de un problema, a la vez que suele generar ideas e hipótesis para una posterior investigación cuantitativa. (atlasti, 2023)

Algunos de los métodos principales de este tipo de investigación son los siguientes:

- Encuestas estandarizadas
- Observaciones estandarizadas
- Experimentos y ensayos
- Análisis de contenido cuantitativo

El diseño de la investigación se compone de lo siguiente:

- Tipo de investigación
- Recogida de datos
- Descripción de los datos
- Método de análisis

El método por el cual se realice la recogida y análisis de los datos adecuados depende de las preguntas de la investigación. En este tipo de investigación se puede distinguir entre variables dependientes e independientes. La investigación cuantitativa, sobre todo el análisis estadístico, es habitual en las ciencias sociales. (atlasti, 2023)

b3. Investigación mixta

De acuerdo con el sitio economipedia, la investigación mixta es aquella que une los métodos cuantitativo y cualitativo, con el fin de disponer de las ventajas de ambos y minimizar sus inconvenientes. (Economipedia, 2021)

Debido a que utiliza los dos métodos, puede conseguir un estudio más completo y detallado sobre un fenómeno determinado. Esta forma de investigar es muy habitual en las ciencias sociales, de la misma forma, es un método muy utilizado en otros campos como la psicología, sociología o economía. (Economipedia, 2021)

Existen varias razones por las cuales se puede llevar a cabo una investigación de este tipo, algunas de ellas son:

- Aprovechar las ventajas de ambos métodos y minimiza sus inconvenientes
- Situaciones en las que el investigador encuentra problemas complejos y que deben ser estudiados en detalle, en estos casos, lo ideal es un análisis previo cuantitativo y escoger una muestra más pequeña a la cual aproximarse cualitativamente.
- Se puede ir de lo particular a lo general, por ejemplo, realizar un experimento en una muestra pequeña, por medio de una investigación exploratoria, y, posteriormente, se lleva a cabo una inferencia en la población.
- Los inconvenientes tienen que ver, sobre todo, con los de los propios métodos utilizados, en este tipo de análisis se pierden detalles de interés, mientras que en el cualitativo no se puede generalizar.

Algunas características de la investigación mixta son:

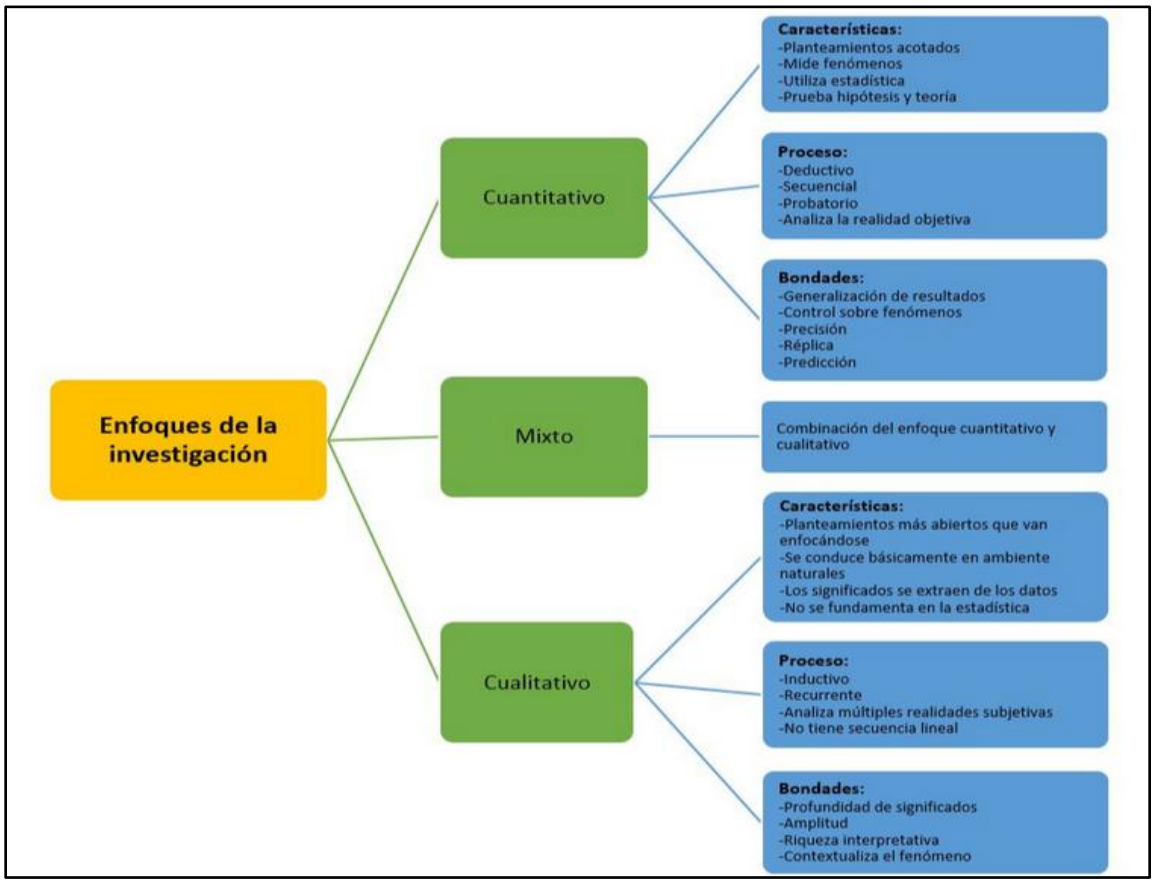
- Es una forma muy completa de obtener información, al unir ventajas de ambos métodos, permite que sea extensa y a su vez detallada.

- Permite complementar el uso de lo cuantitativo, como forma de aproximación, y de lo cualitativo, como forma de análisis en profundidad.
- En este caso, se puede hacer inferencia estadística, a diferencia de lo que sucedía en otras como la explicativa.
- El uso de una metodología mixta permite que se realicen cuestionarios mucho más eficientes, por un lado, basado en escalas como Likert o de tipo dicotómico por otro lado, con planteamientos abiertos que permitan conocer opiniones del entrevistado.

En la siguiente imagen obtenida del sitio recursos.ucol.mx, se explica claramente cada uno de los tipos de enfoque y sus características:

Figura 13

Tipos de enfoques



Nota. Fuente (recursos.ucol, 2024)

De acuerdo con las definiciones presentadas, esta investigación se enmarca en el enfoque mixto, pues combina elementos de los métodos cuantitativo y cualitativo para abordar el problema de investigación. Por un lado, busca establecer los beneficios cualitativos de la automatización en los procesos de detección y corrección de vulnerabilidades, evaluando su impacto en la operativa interna y la mejora en los procedimientos. Por otro lado, se pretende realizar un análisis cuantitativo que permita medir indicadores específicos como la cantidad de tarjetas atendidas, el número de servidores abarcados, el porcentaje de atención a vulnerabilidades, y otras métricas relevantes que respalden los resultados obtenidos.

c. Fuentes de información

Una fuente de información se entiende como cualquier instrumento o recurso que pueda servir para satisfacer una necesidad informativa. Su objetivo es facilitar la localización e identificación de documentos, de tal forma que se pueda responder a la pregunta ¿dónde vamos a buscar la información? (Valencia, 2022)

Existen tres grandes tipos de fuentes:

- Primarias: son aquellas que dan una información nueva u original, que no ha sido recogida o recopilada de antemano, principalmente se trata de información que se incluye en monografías o publicaciones seriadas y sus partes, como los capítulos, artículos, etc.
- Secundarias: son las que no tienen como objetivo principal ofrecer información sino indicar qué fuente o documento la puede proporcionar, es decir, facilitan la localización e identificación de los documentos, no contienen información acabada, siempre remiten a documentos primarios, por ejemplo: bibliografías, catálogos, bases de datos, etc.
- Terciarias: es una mezcla entre la fuente primaria y la secundaria, es decir, contiene información que se extrae de fuentes primaria y secundaria, en este sentido, la fuente terciaria tiene como objetivo depurar dicha información, y transmitirla al lector o investigador, normalmente se encuentra en libros de texto, enciclopedias, o portales de Internet en los que se recoge información y se exponen las fuentes de las que se extrae.

c1. Clasificación de fuentes de información según su tipo

De acuerdo con su tipo, existen dos tipos mayores de fuentes de información, las fuentes que se usan para la búsqueda directa de la información y las fuentes que se usan para la localización e identificación del documento.

- Fuentes para la búsqueda directa de información: a este tipo de fuentes se les ha llamado tradicionalmente “fuentes de información inmediata”, se pueden clasificar en fuentes de información primarias y obras de referencia. Las fuentes de información primarias son aquellas que contienen información original, entre estas destacan las monografías y las publicaciones periódicas, en cuanto a las obras de referencia destacan las enciclopedias, los diccionarios especializados, los directorios, los repertorios biográficos y las estadísticas.
- Fuentes para la identificación y localización del documento: también se conocen como referenciales o bien de información directa o inmediata, entre estas tenemos las bibliografías y los catálogos de bibliotecas. (UGR.ES, 2021)

c2. Otros tipos de categoría de fuentes

Los tipos de fuentes de información ayudan a entender de dónde provienen los datos y como han sido tratados. Dependiendo del grado de información o nivel de información que proporcionan, la información en sí misma, así como la institución o autor que respalda dicha información, esta puede dividirse en diferentes fuentes. Conocer el tipo de fuente ayuda a evaluar la credibilidad y relevancia de la información que se está utilizando, mejorando de esta forma la calidad del trabajo, investigación o estudio. (Economipedia, 2021)

Además de las ya conocidas (primaria, secundaria y terciaria) existen otras fuentes de información, que se detallan a continuación:

- Fuente general: ofrece información muy amplia sobre muchos conceptos, muy distintos y diversos, a la vez, ofrece información sobre fechas históricas, entre otra información relacionada (enciclopedias, libros de texto, manuales).
- Fuente especializada: la fuente especializada, a diferencia de la fuente general, ofrece información sobre un concepto concreto, o sobre un determinado campo de estudio o ciencia. (revistas científicas especializadas, manuales sobre alguna materia especializada, portales específicos donde se encuentran datos relacionados con el tema de investigación.
- Fuente digital: es aquella en la que se expone información y se accede a ella, a través de un soporte digital (revistas digitales, periódicos digitales, portales electrónicos en los que se ofrece información).
- Fuente textual o escrita: es aquella en la que la información que recoge se expone a través de escritos y textos en papel (libros, periódicos, manuales, materiales en formato físico).
- Fuente local: es la fuente que ofrece información sobre un asunto que ha ocurrido en el mismo lugar en el que se encuentra la fuente que ofrece la información, así como, en ocasiones, la institución que respalda (un periódico que expone un suceso ocurrido en una ciudad y que es objeto de estudio).
- Fuente nacional: es la fuente en la que la información que se ofrece, y la institución que la respalda, se encuentran integradas en territorio nacional, es decir en el país en el que ha sucedido lo que se expone en la información (ejemplo: un periódico costarricense cuenta lo sucedido en el país, siendo lo sucedido un objeto de estudio)

- Fuente internacional: es la fuente en la que la información que se ofrece y la institución que la respalda, no se encuentran integradas en el territorio nacional, es decir, no están en el país en el que ha sucedido la lo que se expone en la información (ejemplo: el periódico británico Financial Times, que expone lo sucedido en Africa, durante la etapa colonial). (Economipedia, 2021)

Fuentes primarias a utilizar en esta investigación

Para la presente investigación se estarán utilizando la entrevista como una de las fuentes primarias para la recolección de datos, también se utilizarán los datos generados por el tablero Kanvan de atención de vulnerabilidades, generación de reportes de la herramienta RV Tools, para obtener el dato de la cantidad de servidores virtuales entre otras cosas.

Por medio de la entrevista se pretende extraer la información de la perspectiva de las jefaturas y encargados del proceso de atención de vulnerabilidades respecto al funcionamiento actual del proceso y las ventajas que la automatización puede brindarle en todos los sentidos.

Otra de las fuentes primarias a utilizar es la encuesta, esta se aplicará a un grupo especializado de técnicos, que están en contacto con el proceso de detección y corrección de vulnerabilidades en el INS, esto permitirá tener un amplio panorama de la visión tanto del proceso actual, como de lo que puede aportar la automatización de procesos a esta tarea, es una encuesta bastante completa con 30 preguntas estructuradas para obtener información precisa sobre este proceso y que ayudará en la investigación.

Fuentes secundarias para utilizar en esta investigación

Las fuentes secundarias brindan información al investigador, de los registros ya mencionados en fuentes primarias, en este proyecto se hará uso de las siguientes fuentes secundarias:

- Mediante el uso del internet se hará la investigación de las diferentes herramientas y normas existentes en la actualidad para la automatización de procesos en la atención y corrección de vulnerabilidades.
- Mediante el uso de software se harán laboratorios tendientes a probar la eficacia de las herramientas tecnológicas que se proponen para la automatización de procesos.
- Se buscarán diversas opciones para la automatización de procesos que están ligados a la corrección de vulnerabilidades, por ejemplo, en Azure, y en VMware.

La utilización de estas fuentes dará un panorama más claro de lo que se busca en esta investigación y de las herramientas propuestas para automatizar procesos de detección y corrección de vulnerabilidades en la infraestructura tecnológica del INS.

d. Población de la investigación

La población de estudio es un subconjunto de la población general, que se tiene interés en estudiar y que se halla definida en términos de lugar, tiempo y criterios de selección. Si la población de estudio incluye casos de enfermedad deben especificarse los criterios diagnósticos utilizados. (Valencia, 2022)

Siendo así, la población que realmente se va a estudiar, responde a las siguientes preguntas:

- ¿A quién estudiaremos?

- ¿Cuántos individuos necesitaremos?
- ¿Cómo obtendremos la muestra?
- ¿Dónde incluimos a cada individuo?

Existen varias fórmulas para calcular el tamaño de una muestra, una en caso de que no se conozca con precisión el tamaño de la población y la otra es conociendo el tamaño de la población, en la siguiente gráfica se explican ambos casos:

Figura 14

Cálculo de la muestra sin saber la población

Fórmula que aplica en caso que no se conozca con precisión el tamaño de la población:

$$\mathbf{n} = \frac{Z^2 \mathbf{p}\,\mathbf{q}}{E^2}$$

donde:

n es el tamaño de la muestra;

Z es el nivel de confianza;

p es la variabilidad positiva o probabilidad de éxito;

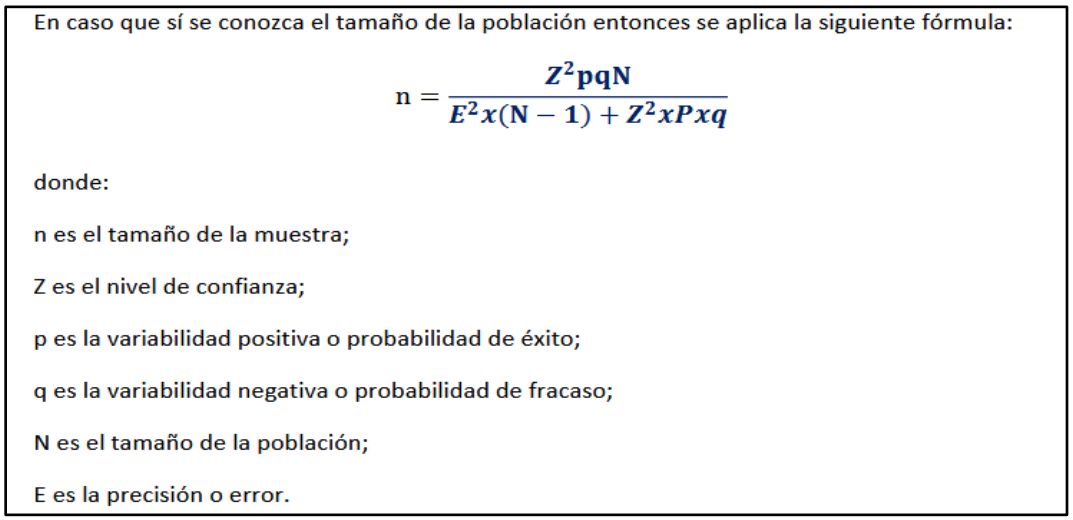
q es la variabilidad negativa o probabilidad de fracaso;

E es la precisión o error.

Nota. Fuente: (INA, 2023)

Figura 15

Cálculo de la muestra conociendo la población



Nota. Fuente: (INA, 2023)

d1. Tipos de población

Una población es un conjunto completo de individuos u objetos que comparten características similares. La población puede comprender una nación o un grupo de personas u objetos con una característica común, incluye a todo el grupo bien definido sobre el que cualquier investigación quiere extraer conclusiones. (QuestionPro, 2022)

Existen diferentes tipos de poblaciones, a saber:

Población Diana: se refiere a todo el grupo de individuos u objetos a los que los investigadores están interesados en generalizar las conclusiones. La población diana suele tener características variables y también se conoce como población teórica. (QuestionPro, 2022)

Población accesible: es la población de la investigación a la que los investigadores pueden aplicar sus conclusiones. Esta población es un subconjunto de la población objetivo y

también se conoce como población de estudio. Los investigadores extraen sus muestras de la población accesible. (QuestionPro, 2022)

El tamaño y la densidad son las medidas más importantes para describir el estado actual de una población y, potencialmente, para hacer predicciones sobre cómo podría cambiar en el futuro.

El tamaño de la población es el número de individuos que la componen, es decir, el número total de personas representativas de una población específica en un período determinado.

La densidad de la población es el número medio de individuos por unidad de superficie o volumen, es decir, es un número medio que se calcula dividiendo el número de personas por la superficie. (QuestionPro, 2022)

d2. Representación gráfica de la población

Existen 7 formas de representar gráficamente la población:

- Gráficos de barras: suelen utilizarse para mostrar el crecimiento de la población a lo largo del tiempo, pero también pueden mostrar aspectos diversos, como las proporciones relativas de los distintos grupos de la sociedad o bien, pueden utilizarse para comparar poblaciones de distintos lugares.
- Gráficos lineales: se utilizan para mostrar el crecimiento de la población a lo largo de un período de tiempo. La atención no se centra tanto en el valor de cada punto del gráfico como en la tendencia de crecimiento que refleja el panorama general de aumento o disminución de la población.
- Gráficos circulares: se utilizan para comparar las proporciones relativas de grupos dentro de una población, como los distintos grupos étnicos. La atención no se

centra en el tamaño total de una población, sino en qué proporción de ese total representa cada grupo.

- Pictogramas: los pictogramas utilizan la imagen para mostrar datos, el uso de figuras ayuda al lector a “humanizar” los datos representados. Cada “persona” de este gráfico representa un número determinado.
- Mapas de puntos: son imágenes que muestran cómo está distribuida la población en una zona geográfica. Un punto representa un número concreto de personas, por lo que más puntos significan mayor densidad de población en una zona.
- Mapas choropleth: estos mapas utilizan el sombreado para mostrar las diferentes densidades de población de una zona. Los tonos más oscuros representan mayores concentraciones de personas en una región específica, aquí lo importante no es el número real de personas, sino donde se concentran.
- Gráfico piramidal: el gráfico piramidal se considera la mejor forma de ilustrar gráficamente la distribución por edad y sexo de una población determinada. El gráfico piramidal o pirámide de población utiliza un gráfico de barras pareadas y muestra el número o porcentaje de hombres y mujeres en cada grupo de edad. Son tipos especiales de gráficos que muestran cómo está constituida una población determinada en función del sexo y la edad. (QuestionPro, 2022)

d3. Formas de muestreo de la población

Existen diversas formas de muestrear la población, se explican algunas de ellas a continuación:

- Muestreo aleatorio simple: cada individuo se elige al azar y cada miembro de la población tiene la misma posibilidad, o probabilidad, de ser seleccionado.
- Muestreo sistemático: los individuos se seleccionan a intervalos regulares a partir del marco de muestreo.
- Muestreo estratificado: la población se divide primero en subgrupos (o estratos) que comparten una característica similar.
- Muestreo por conglomerados: se utilizan subgrupos de la población como unidad de muestreo, en lugar de individuos, aquí la población se divide en subgrupos, denominados conglomerados.
- Muestreo por conveniencia: es el tipo de muestreo más sencillo, pues los participantes se seleccionan en función de su disponibilidad y voluntad de participar.
- Muestreo de bola de nieve: se utiliza habitualmente en ciencias sociales para investigar grupos de difícil acceso, aquí se pide a los sujetos existentes que recomienden a otros sujetos conocidos por ellos de modo que la muestra aumenta de tamaño como una bola de nieve rodante.
- Muestreo de juicio: también se conoce como muestreo selectivo o subjetivo, se basa en el juicio del investigador a la hora de elegir a quién se pide que participe. De esta forma se puede elegir una muestra “representativa” que se ajuste a las necesidades, o dirigirse específicamente a personas con determinadas características. (QuestionPro, 2022)

En la presente investigación, por su naturaleza, se estará utilizando el tipo de muestreo de juicio, pues la población a la cual va dirigida la entrevista es bastante limitada y especializada en el tema.

e. Variables y unidades de análisis

Una variable representa cualquier característica, número o cantidad que puede medirse o cuantificarse. El término engloba cualquier cosa que pueda variar o cambiar, desde conceptos simples como la edad y la altura hasta otros más complejos como el nivel de satisfacción o la situación económica. Las variables son esenciales en la investigación, pues son elementos fundamentales que los investigadores manipulan, miden o controlan para comprender mejor las relaciones, las causas y los efectos de sus estudios. Permiten plantear preguntas de investigación, formular hipótesis e interpretar resultados. (atlasti, 2023)

e.1.Tipos de variables

Existen 5 tipos de variables en investigación, las cuales se describen a continuación:

Variables independientes

Son fundamentales para la estructura de la investigación, pues sirven como factores o condiciones que los investigadores manipulan o varían para observar sus efectos sobre las variables dependientes. Se consideran independientes porque su variación no depende de otras variables del estudio. En cambio, son la causa o el estímulo que influye directamente en los resultados que se miden. (atlasti, 2023)

Variables dependientes

Son los resultados o efectos que los investigadores pretenden explorar y comprender en sus estudios. Estas variables se denominan de esta forma porque sus valores dependen de los cambios o variaciones de las variables independientes. Básicamente son las respuestas o resultados que se miden para evaluar el impacto de la manipulación de la variable independiente.

Su medición e identificación son cruciales para comprobar la hipótesis y extraer conclusiones de la investigación. Permite que los investigadores puedan cuantificar el efecto de la variable independiente, aportando pruebas de relaciones o asociaciones causales. (atlasti, 2023)

Variables categóricas

Son también conocidas como variables cualitativas, representan tipos o categorías que se utilizan para agrupar observaciones. Dividen los datos en grupos o categorías distintos que carecen de valor numérico pero que tienen un significado importante en la investigación. Algunos ejemplos son el sexo, el tipo de vehículo, el estado civil. Estas categorías ayudan a los investigadores a organizar los datos en grupos para su comparación y análisis.

Se pueden clasificar en dos subtipos: nominales y ordinales. Las nominales son categorías sin ningún orden o clasificación inherente entre ellas, como el grupo sanguíneo o la etnia. Las variables ordinales, en cambio, implican una especie de clasificación u orden entre las categorías, como los niveles de satisfacción (alto, medio, bajo) o el nivel educativo (bachillerato, licenciatura, máster, doctorado). (atlasti, 2023)

Variables continuas

Son variables cuantitativas que pueden tomar un número infinito de valores dentro de un rango determinado. Estas variables se miden a lo largo de un continuo y pueden representar mediciones muy precisas. Algunos ejemplos de variables continuas son la altura, el peso, la

temperatura y el tiempo. Dado que puede asumir cualquier valor dentro de un intervalo, las variables continuas permiten un análisis detallado y un alto grado de precisión en los resultados de la investigación. La precisión de las variables continuas mejora la capacidad del investigador para detectar patrones, tendencias y relaciones causales en los datos. (atlasti, 2023)

Variables de confusión

Son aquellas que pueden causar una asociación falsa entre las variables independientes y dependientes, lo que puede llevar a conclusiones incorrectas sobre la relación estudiada. Se trata de variables extrañas que no se tuvieron en cuenta en el diseño del estudio pero que pueden influir tanto en la supuesta causa como en el efecto, creando una correlación engañosa. Abordar adecuadamente las variables de confusión refuerza la credibilidad de los resultados de la investigación al aclarar la relación directa entre las variables dependientes e independientes, proporcionando así resultados más precisos y fiables. (atlasti, 2023)

En esta investigación, se estarán utilizando variables tanto dependientes como independientes, y en cierto punto variables categóricas, pues los valores a medir son muy específicos.

f. Métodos de investigación

Los métodos de investigación son los distintos modelos de procedimientos que se pueden emplear en una investigación específica, atendiendo a las necesidades de esta, o sea, la naturaleza del fenómeno que se desea investigar. Un ejemplo perfecto es el método científico, una serie de procedimientos de tipo lógico y experimental que permiten comprobar una hipótesis mediante experiencias controladas, replicables y precisas. (concepto, 2021)

f1. Tipos de métodos de investigación

Los métodos de investigación se clasifican en lógicos y en empíricos. Los métodos lógicos de investigación implican la utilización del pensamiento y el razonamiento para ejecutar deducciones, análisis y síntesis.

Por otro lado, los métodos empíricos de investigación se aproximan al conocimiento mediante experiencias replicables, controladas y documentadas, conocidos bajo el nombre de experimentos.

Algunos de los tipos de métodos más conocidos son:

- Método lógico-deductivo: consiste en aplicar principios generales a casos particulares, a partir de ciertos enlaces de juicios.
- Método deductivo directo: empleado sobre todo en la lógica y el razonamiento formal, extrae de un conjunto finito de premisas comprobadas una conclusión única y verdadera.
- Método deductivo indirecto: es el método basado en la lógica del silogismo, es decir, de la comparación de dos premisas iniciales para obtener una conclusión.
- Método hipotético deductivo: se trata del método que parte de una hipótesis o explicación inicial, para luego obtener conclusiones particulares de ella, que luego serán a su vez comprobadas experimentalmente.
- Método lógico inductivo: propone el camino inverso: a partir de premisas particulares, se infieren conclusiones universales o generales, ya sea mediante inducciones completas o incompletas.

En la presente investigación se utilizará el método hipotético deductivo, pues basado en los datos actuales de la atención de vulnerabilidades, se estará proponiendo y probando herramientas tecnológicas que puedan mejorar esos datos.

g. Tabla de operacionalización de variables

Tabla 2

Tabla de operacionalización de variables

Objetivo	Variable	Dimensión	Indicadores	Instrumentos de recolección de datos
General: Proponer un modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológica del INS para optimizar los	Modelo Automatizado para la detección y corrección de vulnerabilidades	-Eficiencia del modelo	Tiempo de respuesta en la detección/corrección de vulnerabilidades	Análisis documental

procesos de seguridad y minimizar los riesgos asociados a los ciberataques.				
		-Cumplimiento de estándares de ciberseguridad.	-Porcentaje de cumplimiento con estándares internacionales	-Entrevistas con expertos.
		-Integración con infraestructura tecnológica actual	-Nivel de integración tecnológica alcanzado	-Pruebas piloto del modelo.
Específico 1: Examinar los procesos actuales utilizados por	Procesos actuales del departamento de Operación y	-Diagnóstico situacional	-Número de procesos relacionados con la detección/correcció	-Entrevistas

el departamento de Operación y Soporte Técnico para identificar oportunidades de mejora.	Soporte Técnico.		n de vulnerabilidades	
		- Identificación de brechas	-Brechas detectadas respecto a mejores prácticas	-Encuestas a personal técnico -Observación directa.
Específico 2: Identificar los requerimientos y especificaciones técnicas necesarias para desarrollar un modelo optimizado.	Requerimientos y especificaciones técnicas	-Normativas y estándares aplicables	-Número de estándares identificados	-Análisis documental de estándares.

		-Herramientas tecnológicas	-Especificaciones técnicas detalladas	-Consulta a especialistas en ciberseguridad.
			-Herramientas seleccionadas y sus características.	
Específico 3: Elaborar una propuesta de automatización de procesos para integrar metodologías ágiles y herramientas tecnológicas avanzadas.	Propuesta de automatización de procesos	-Metodologías ágiles	-Metodologías ágiles identificadas e implementadas	-Revisión de herramientas disponibles
		-Herramientas tecnológicas avanzadas	-Herramientas seleccionadas para la automatización	- Encuestas/entrevistas con personal clave.

		-Impacto esperado	-Mejora en indicadores de seguridad	-Pruebas de concepto o simulaciones.

h. Recolección de datos

La recolección de datos es el proceso de búsqueda, recolección y medición de datos de diferentes fuentes para obtener información sobre los procesos, servicios y productos de una empresa o negocio y evaluar dichos resultados y así se puedan tomar mejores decisiones. (maestriasydiplomadostec, 2023)

La recolección de datos sirve para mejorar los procesos de mejora continua, pero se debe entender que también depende en gran medida del problema que esté atacando u objetivo planteado por el cual se está realizando dicha recolección.

h1. Técnicas para recolección de datos

Algunas de las técnicas más utilizadas para la recolección de datos son las siguientes:

Observación

La observación consiste en saber seleccionar aquello que se desea analizar. Para la observación lo primero es plantear previamente qué es lo que interesa observar, en definitiva, haber seleccionado un objetivo claro de observación. La observación científica tiene la capacidad de describir y explicar el comportamiento, al haber obtenido datos adecuados y fiables correspondientes a conductas, eventos y /o situaciones perfectamente identificadas e insertas en un contexto teórico. (UGR.ES, 2021)

Observación Naturalista

Es un método de investigación utilizado en las ciencias sociales y en la biología para recopilar datos mediante la observación directa y sistemática de fenómenos naturales en su entorno real. Se basa en la idea de estudiar el comportamiento y las interacciones de los sujetos de estudio en su ambiente natural, sin intervenir ni manipular intencionalmente el entorno. (QuestionPro, 2022)

Observación estructurada

Es un método sistemático y predeterminado de recopilación de datos que implica observar y registrar comportamientos o eventos específicos. Este método requiere un plan de observación detallado con categorías y criterios predefinidos para registrar las observaciones. (fastercapital, 2022)

Observación participante

La observación participante es la investigación que involucra la interacción social entre el investigador y los informantes en el milieu (escenario social, ambiente o contexto) de los últimos y durante la cual se recogen datos de modo sistemático y no intrusivo. Implica la selección del escenario social, el acceso a ese escenario, normalmente una organización o institución, la interacción con los porteros y con los informantes y la recolección de datos. (Jaen, 2023)

Observación no participante

Es aquella en la cual se recoge la información desde afuera, sin intervenir para nada en el grupo social, hecho o fenómeno investigado. Es un método que se está aplicando en muy distintas disciplinas, ha sido más frecuente en las ciencias sociales, sobre todo, en la sociología y la antropología, su finalidad es clara y presuntamente lógica que es promover y salvaguardar la mayor objetividad posible. (VIU, 2022)

Observación directa

Es un método de recolección de datos que consiste básicamente en observar el objeto de estudio dentro de una situación particular. Todo esto se hace sin necesidad de intervenir o alterar el ambiente en el que se desenvuelve el objeto. De lo contrario los datos que se obtienen no serán válidos. Este método se usa en ocasiones en las que otros sistemas, como pueden ser las encuestas, cuestionarios, entre otros, no son tan efectivos. Se recomienda recurrir a la observación directa cuando lo que se quiere es evaluar el comportamiento por un período de tiempo continuo. (QuestionPro, 2022)

Observación indirecta

La observación indirecta es un tipo de observación en el que el investigador no observa directamente el comportamiento de los sujetos o eventos que está estudiando, sino que utiliza registros previamente existentes, como documentos, archivos, registros de audio o video, fotografías u otras formas de información.

Este tipo de observación puede proporcionar acceso a información que de otra manera sería difícil o imposible de obtener a través de observación directa o entrevistas. En segundo lugar, puede permitir una comparación entre diferentes períodos de tiempo o diferentes grupos de sujetos, lo que puede ser útil para identificar patrones y tendencias. (QuestionPro, 2022)

Observación encubierta

En este tipo de observación, el investigador se infiltra en el grupo que está siendo observado sin que los miembros del grupo lo sepan. Este tipo de observación plantea cuestiones éticas y es poco común en la investigación científica.

La observación encubierta plantea cuestiones éticas importantes, pues se considera una invasión de la privacidad de los sujetos. En muchos casos, es necesario obtener el consentimiento informado de los sujetos antes de llevar a cabo la observación encubierta, y el investigador debe

equilibrar los beneficios potenciales de la investigación con los posibles efectos negativos para los sujetos involucrados. (QuestionPro, 2022)

Cuestionarios o encuestas

Un cuestionario es un conjunto de preguntas escritas utilizadas para obtener información indistintamente para evaluar a una sola persona. Aun cuando el cuestionario puede ser respondido por más de una persona, las respuestas no forman parte de un análisis estadístico.

Una encuesta agrega datos específicos a los cuestionarios para que al finalizar pueda existir un análisis estadístico con la información obtenida para evaluar a un grupo de personas, pues las respuestas se agregan para llegar a una conclusión. (QuestionPro, 2022)

Focus Group

El término focus Group fue inventado por el experto en marketing y psicología Ernest Ditcher, este término describe reuniones celebradas con un grupo limitado de participantes con el objetivo de debatir. (QuestionPro, 2022)

Actualmente siguen siendo uno de los métodos más utilizados para la investigación, sobre todo si de investigación cualitativa se trata. Su uso frecuente se da, por lo regular, por la sencillez de esta técnica que permite conocer de manera rápida lo que piensan las personas del tema en cuestión.

Esta metodología debe llevarse a cabo de manera precisa para lograr los resultados deseados, para ello se necesita también que participen activamente sus miembros, a fin de que proporcionen toda la información. (QuestionPro, 2022)

Entrevistas

La entrevista es un método de recolección de datos primarios que consiste en preguntar a una o varias personas su opinión sobre una empresa, un producto o un tema. Tienen un carácter

cualitativo por lo que se centran en la experiencia personal. El objetivo principal de las entrevistas es conocer los comportamientos, actitudes y opiniones de las personas, suelen tener un mayor índice de respuesta y proporcionan resultados más fiables. (QuestionPro, 2022)

Formularios de contacto

Un formulario de contacto es un área de un sitio web en la que pueden llenarse distintos campos que permiten al usuario ponerse en contacto con una empresa y se caracteriza por ser una herramienta clave que impulsa la página a generar una comunicación más directa con clientes y prospectos sin importar que estos se encuentran a larga distancia. (QuestionPro, 2022)

Fuentes abiertas

Una fuente abierta no es solamente todo aquello que se circunscribe al ámbito de internet. Aunque hoy en día, la era de las tecnologías de la información y la comunicación, casi todos accedemos a través de internet, las fuentes abiertas no solo existen en este ámbito. (OpenWebinars, 2024)

Las fuentes abiertas son de carácter público:

- Con independencia de que el contenido se comercialice
- Con independencia del soporte
- Con independencia del medio de transmisión
- Con independencia del modo de acceso

Algunos ejemplos de fuentes abiertas serían una enciclopedia, una legislación, un anuario, una publicación científica, un canal RSS, un blog, una conferencia de prensa, una retransmisión de radio, una retransmisión de televisión, etc. (OpenWebinars, 2024)

Monitoreo de redes sociales

Consiste en rastrear, analizar y recopilar información de las diferentes plataformas sociales. Esta información puede incluir menciones a una marca, hashtags, palabras clave, opiniones de clientes, tendencias del mercado y mucho más. (UNIR, 2024)

Las claves principales del monitoreo de redes sociales son:

- Definir detalladamente los objetivos y KPIs en redes sociales
- Elegir las plataformas más relevantes para cada empresa
- Buscar las palabras clave, hashtags y los temas de interés
- Segmentar la monitorización
- La constancia y la toma de decisiones

Análisis de sitio web

El análisis de un sitio web implica observar el rendimiento de esta y realizar mejoras para generar más clientes potenciales e ingresos. Se pueden analizar diferentes áreas de rendimiento, desde la clasificación en los resultados de búsqueda hasta la velocidad de carga de un sitio web. (QuestionPro, 2022)

Un análisis de sitio web se puede realizar de la siguiente manera:

- Determinar lo que se desea analizar
- Documentar los resultados ideales
- Analizar los datos
- Encontrar áreas de mejora
- Analizar el sitio web periódicamente

Historial de conversaciones

La herramienta de historial de conversaciones proporciona una interfaz para explorar y analizar conversaciones de producción reales entre un agente y los usuarios finales. Esto puede

ser útil para evaluar el rendimiento funcional de tu agente o para depurar problemas. (google, 2025)

Revisión documental

Es una técnica de investigación cualitativa que se encarga de recopilar y seleccionar información a través de la lectura de documentos, libros, revistas, grabaciones, filmaciones, periódicos, bibliografías, etc.

A comparación de otros métodos, la investigación documental no es tan popular debido a que las estadísticas y cuantificación están consideradas como formas más seguras para el análisis de datos. Este tipo de investigación suele asociarse con la investigación histórica, por lo que los investigadores pierden confianza por su falta de claridad. Sin embargo, la historia da sentido al pasado y al presente.

i. Procesamiento de datos de la investigación:

El procesamiento de datos en la investigación es el proceso de recopilación de datos y su transformación en información utilizable para múltiples partes interesadas. Aunque los datos pueden verse de muchas maneras y a través de varios objetivos, el procesamiento de datos ayuda a probar o refutar teorías, a tomar decisiones empresariales o incluso a avanzar en la mejora de productos y servicios. El procesamiento de datos se utiliza incluso en la investigación para entender los sentimientos de los precios, el comportamiento y las preferencias de los consumidores y el análisis de la competencia. (QuestionPro, 2022)

i.1. Pasos del procesamiento de datos en la investigación

El procesamiento de datos en la investigación tiene seis pasos, a continuación, se detallan los pasos:

Recolección de datos de la investigación

Es la etapa principal del proceso de investigación. Este proceso puede realizarse a través de diversas técnicas de investigación online y offline y puede ser una mezcla de métodos de investigación primarios y secundarios. La forma de recogida de datos más utilizada son las encuestas de investigación, también se pueden recopilar datos a través de grupos de discusión, módulos de debate, etc. (QuestionPro, 2022)

Preparación de los datos de la investigación

Es el segundo paso, es la preparación de los datos para eliminar las incoherencias, eliminar los datos malos o incompletos de la encuesta y limpiar los datos para mantener el consenso. (QuestionPro, 2022)

Introducción de los datos de la investigación

El siguiente paso consiste en introducir los datos depurados en un formato legible digitalmente y coherente con las políticas de la organización, las necesidades de la investigación, etc. Este paso es fundamental, pues los datos se introducen en sistemas en línea compatibles con la gestión de datos de investigación. (QuestionPro, 2022)

Procesamiento de los datos de investigación

Una vez introducidos los datos en los sistemas, es fundamental procesarlos para darles sentido. La información se procesa en función de las necesidades, los tipos de datos recogidos, el tiempo disponible para procesar los datos y otros muchos factores. Este es uno de los componentes más críticos del proceso de investigación. (QuestionPro, 2022)

Salida de los datos de la investigación

En esta etapa del procesamiento de los datos de la investigación es donde se convierten en conocimientos. Esta etapa permite a los propietarios de las empresas, a las partes interesadas y

al resto del personal ver los datos en forma de gráficos, tablas, informes y otros formatos fáciles de consumir. (QuestionPro, 2022)

Almacenamiento de los datos de investigación procesados

La última etapa de los pasos del procesamiento de datos es el almacenamiento. Es esencial mantener los datos en un formato que se pueda indexar, buscar y crear una única fuente de verdad. Las plataformas de gestión del conocimiento son las más utilizadas para el almacenamiento de los datos de investigación procesados. (QuestionPro, 2022)

j. Instrumentos para la recolección de datos

La recolección de datos es un proceso esencial en cualquier organización que busca tomar decisiones informadas y estratégicas. Este proceso implica la recopilación sistemática de información que puede ser analizada y utilizada para mejorar procesos, productos y servicios.

La recolección de datos es fundamental en la investigación científica, estudios de mercado, análisis de comportamiento del consumidor y en la mejora de la eficiencia operativa. (clientify, 2024)

Existen varios métodos de recolección de datos, a saber:

j.1.Métodos cualitativos

Entrevistas

Las entrevistas permiten obtener información detallada y profunda directamente de las personas. Son útiles para explorar opiniones, experiencias y percepciones. (QuestionPro, 2022)

Grupos focales

Los grupos focales reúnen a un pequeño grupo de personas para discutir un tema específico. Este método es valioso para obtener múltiples perspectivas en un entorno interactivo. (QuestionPro, 2022)

Observación participante

Implica que el investigador se involucre directamente en el entorno que está estudiando., Esta técnica es útil para obtener una comprensión profunda del comportamiento y las interacciones en un contexto natural. (QuestionPro, 2022)

j.2.Métodos cuantitativos

Encuestas

Son herramientas populares para recolectar datos de un gran número de personas. Permiten obtener información cuantificable que puede ser analizada estadísticamente. (QuestionPro, 2022)

Experimentos

Los experimentos controlados son utilizados para probar hipótesis específicas mediante la manipulación de variables y la observación de los resultados. (QuestionPro, 2022)

Análisis de registros

El análisis de registros implica revisar y analizar datos ya existentes, como informes financieros, registros de ventas y datos de clientes. Esta técnica es eficaz para identificar tendencias y patrones históricos. (QuestionPro, 2022)

k. Técnicas para el análisis de datos

Las técnicas para el análisis de datos se eligen dependiendo del objeto de estudio, a continuación, se describen los más importantes de acuerdo con (atlasti, 2023):

k.1.Análisis de datos descriptivos

El objetivo de este tipo de análisis es describir los datos encontrados en una muestra mediante valores característicos y presentarlos en forma de gráfico o tabla. Esta presentación de los datos se refiere a las variables individuales y a sus características.

k.2.Análisis de datos exploratorio

El análisis de datos exploratorio o la estadística exploratoria es una rama de la estadística, examina y valora los datos de los que se tiene poco conocimiento sobre sus relaciones, muchas técnicas de este tipo de análisis se utilizan en la minería de datos.

k.3.Análisis de datos predictivo

Este tipo de análisis incluye una serie de técnicas estadísticas de minería de datos, modelización predictiva y aprendizaje automático. Los datos actuales e históricos se analizan para hacer predicciones sobre eventos futuros.

k.4.Análisis de datos de diagnóstico

Este tipo de análisis de diagnóstico aborda específicamente la cuestión de por qué ha ocurrido algo. Mediante la comparación de datos históricos y de otro tipo, la identificación de patrones y el descubrimiento de relaciones, encuentra las causas o las interacciones mutuas.

k.4.Análisis de datos prescriptivo

Es la categoría de análisis más compleja y costosa, aporta un gran valor añadido al responder a la pregunta de investigación, como, por ejemplo, cómo alcanzar los objetivos fijados, este tipo de análisis se basa en datos históricos y actuales procedentes de fuentes de datos internas y externas.

l. Herramientas de análisis de datos

De acuerdo con el sitio especializado QuestionPro (QuestionPro, 2022), las herramientas de análisis de datos son aquellas que ayudan a gestionar los datos que se adquieren a lo largo de un estudio o provenientes de un negocio. Se utilizan para desarrollar y supervisar prácticas y organizar, procesar y analizar datos.

Las herramientas de análisis de datos también ayudan a proteger la privacidad y la seguridad y a eliminar los datos duplicados. Una gestión de datos eficaz controla y organiza los datos mediante una combinación de herramientas de software y buenas prácticas.

Las herramientas de gestión de datos se pueden dividir en cuatro grandes categorías:

- Herramientas de análisis de datos en la nube
- Herramientas ETL y de integración de datos
- Herramientas de análisis de datos maestros (MDM)
- Herramientas de visualización y análisis de datos

Las características que deben tener las herramientas de análisis de datos son las siguientes:

- Flexibilidad
- Instalaciones basadas en la nube
- Optimización de datos
- Seguridad

l.1.Visualización de datos

De acuerdo con IBM (2024), la visualización de datos es la representación de datos mediante el uso de gráficos comunes, como diagramas, gráficas, infografías e incluso

animaciones. Estas pantallas visuales de información comunican relaciones de datos complejas e insights basados en datos de una manera fácil de entender.

l2. Análisis de agrupamientos

Consiste en reunir elementos a partir de las características que comparten, con el propósito de realizar una evaluación profunda comparando los resultados obtenidos con la selección a la que pertenece cada elemento. En las encuestas, por ejemplo, este análisis permite que el investigador ordene las respuestas basándose en los parámetros establecidos, estos grupos pueden ser de tiempo, tipo de respuesta, ubicación, etc. (QuestionPro, 2022)

l3. Análisis de tendencias

Es un análisis que brinda la posibilidad de ver datos a lo largo del tiempo en el que se está llevando a cabo una encuesta, sobre todo si es una encuesta a largo plazo. Puede ser útil para comparar las puntuaciones de las pruebas o exámenes o para identificar tendencias para una encuesta de satisfacción que se distribuye regularmente. (QuestionPro, 2022)

l.4.Análisis de textos

Es el proceso en el cual se utilizan los sistemas de computación para leer y comprender texto escrito por seres humanos y así, obtener información empresarial. Un software de este tipo puede, de forma independiente, clasificar, ordenar y extraer información de distintos textos para identificar patrones, relaciones, opiniones y otra información que se pueda procesar. (aws, 2024)

La importancia de este tipo de análisis radica en que permite a las empresas que lo utilizan, extraer información procesable de varios orígenes de datos sin estructura.

l.5. Minería de datos

Es el uso del machine learning y el análisis estadístico para descubrir patrones y otra información valiosa a partir de grandes conjuntos de datos. Dada la evolución del Machine

Learning, el almacenamiento de datos y el crecimiento del big data, la adopción de la minería de datos, también conocida como descubrimiento de conocimientos en base de datos (KDD), se ha acelerado rápidamente en las últimas décadas.

Las técnicas de minería de datos que sustentan los análisis de datos se pueden implementar para dos propósitos principales. Pueden describir el conjunto de datos objetivo o pueden predecir resultados mediante el uso de algoritmos de machine learning. (IBM, 2023)

l.6. Benchmark

El benchmark es un punto de referencia usado para medir el rendimiento de una inversión. Es un indicador financiero que sirve para comparar y evaluar cómo está yendo una inversión en comparación con otras.

Es una palabra de origen inglés y significa “punto de referencia” o “parámetro”, es también utilizada en marketing para comparar un producto o técnica exitosa. (Economipedia, 2021)

Definición de instrumentos de recolección de datos para la investigación

Para satisfacer las necesidades planteadas en el tema “Automatización del Proceso de Detección y Corrección de Vulnerabilidades en la Infraestructura Tecnológica del Instituto Nacional de Seguros (INS)”, es necesario utilizar instrumentos de recolección de datos que permitan obtener información precisa y relevante sobre el estado actual de la infraestructura tecnológica, las prácticas de seguridad, las vulnerabilidades existentes y las posibles áreas de mejora. Los instrumentos de recolección de datos deben ser capaces de capturar información cualitativa y cuantitativa que permita realizar un diagnóstico detallado de la situación y, a partir

de ahí, diseñar un modelo automatizado eficaz. A continuación, se proponen varios instrumentos adecuados para esta investigación:

Entrevistas con personal clave del INS

Las entrevistas estructuradas o semiestructuradas con los responsables de la infraestructura tecnológica, seguridad informática, y operaciones del INS son fundamentales para obtener información detallada sobre los procesos actuales de gestión de vulnerabilidades y los desafíos que enfrentan. Estas entrevistas pueden proporcionar datos cualitativos clave sobre los procedimientos actuales, la efectividad de las herramientas utilizadas y la percepción sobre la necesidad de una automatización.

El objetivo de realizar estas entrevistas es el de obtener un panorama más amplio desde todas las funciones principales en TI, de lo que se realiza actualmente, de lo que se planea realizar, del conocimiento de la automatización y la percepción que se tiene de esta, por lo tanto, se estarán realizando a los siguientes roles:

- Director de TI
- Encargado del área de seguridad de TI
- Jefatura del Departamento de Operaciones y Soporte Técnico
- Encargado unidad de redes
- Encargado de área Aplicaciones Nube-Tierra
- Encargado de proceso de atención de vulnerabilidades

Encuestas a usuarios y administradores de sistemas

Las encuestas son una herramienta útil para recolectar datos cuantitativos sobre las prácticas actuales de gestión de vulnerabilidades y la disposición del personal a adoptar un

modelo automatizado. Las encuestas pueden dirigirse a usuarios finales, administradores de sistemas, y otros actores involucrados en la seguridad de la infraestructura tecnológica.

El objetivo de las encuestas es el de conocer de primera mano la información de los equipos involucrados en la administración de los servidores, así como de los funcionarios miembros de la llamada Célula Chirripó, que se encarga de la atención y corrección de vulnerabilidades, así como, a los funcionarios de la unidad de Seguridad de TI que se encargan de los escaneos que nutren a la Célula y de la seguridad informática en general, esto permitirá tener un panorama claro de la percepción, conocimiento y utilización que estos funcionarios tienen y hacen de las herramientas automatizadas para la detección y corrección de vulnerabilidades.

Análisis de documentación interna

Revisar la documentación existente sobre las políticas de seguridad, protocolos de gestión de vulnerabilidades, informes de auditoría de seguridad y cualquier otro material relevante que detalle los procedimientos y normativas de ciberseguridad del INS. Esto proporcionará un panorama claro de las metodologías, herramientas y recursos disponibles para la gestión de vulnerabilidades.

El objetivo de este análisis es contar con los insumos necesarios y el conocimiento respecto a los lineamientos actuales en materia de ciberseguridad en el INS, además contar con datos exactos y actuales en lo que se refiere a detección y corrección de vulnerabilidades y todas las estadísticas con las que se pueda contar, esto permitirá establecer algún tipo de comparativa con las herramientas que se propongan en esta investigación.

Las fuentes de las cuales se estará obteniendo esta información son las siguientes:

- Procedimientos internos de seguridad de TI

- Informes de Auditoría en materia de seguridad informática
- Políticas internas de seguridad de TI
- Reportes obtenidos del tablero Kanvan utilizado por el grupo Chirripó
- Reportes obtenidos por el área de seguridad de TI obtenidos de la herramienta Nessus

Análisis de herramientas tecnológicas utilizadas

Para obtener una comprensión precisa de las herramientas y tecnologías que el INS emplea en la gestión de vulnerabilidades, se puede utilizar un análisis de herramientas de seguridad existentes, como sistemas de gestión de parches, escaneos de vulnerabilidades, sistemas de detección de intrusiones (IDS), y las plataformas de gestión de incidentes de seguridad.

Si bien es cierto estos datos se extraerán de las entrevistas y encuestas, actualmente se cuentan con las siguientes herramientas que serán analizadas:

- Nessus (escaneo de vulnerabilidades)
- Kanvan (tablero de atención de tarjetas de vulnerabilidades)
- Microsoft Azure
- Aranda (gestión de incidentes)

Revisión de resultados de escaneos de vulnerabilidades

El análisis de los resultados de escaneos de vulnerabilidades previos, ya sean internos o externos, proporcionará datos sobre las debilidades específicas de la infraestructura tecnológica del INS. Esto permitirá identificar patrones, áreas de alta prioridad y posibles procesos manuales que podrían beneficiarse de la automatización.

Esta revisión será realizada en conjunto con los funcionarios del área de Seguridad de TI, que cuentan con el acceso a los datos de la herramienta Nessus.

Estudio de caso de otras organizaciones

Revisar y analizar casos de otras organizaciones, especialmente aquellas en el sector financiero o en seguros, que hayan implementado modelos automatizados para la detección y corrección de vulnerabilidades. Esto puede proporcionar ideas sobre las mejores prácticas y tecnologías efectivas.

Es importante notar en este sentido, que la información en este aspecto es muy delicada, por lo tanto, esto puede suponer una limitante a la hora de obtener datos, esto, porque es probable que dicha información no sea pública y sea de difícil acceso. Además, se debe considerar que en el sector seguros debido a la competencia existente no será posible obtener datos que no sean públicos.

Análisis de benchmarking de normas internacionales aplicables

El análisis de benchmarking de normas internacionales es un paso crucial para desarrollar un modelo automatizado de detección y corrección de vulnerabilidades, pues permite evaluar y adoptar las mejores prácticas, estándares y marcos de trabajo en el ámbito de la ciberseguridad.

Al analizar las normativas internacionales, se garantiza que el modelo propuesto no solo cumpla con las expectativas y necesidades del Instituto Nacional de Seguros (INS), sino que también se adhiera a las mejores prácticas de seguridad reconocidas globalmente.

Se analizarán y crearán cuadros comparativos de las siguientes normativas para evaluar su aplicabilidad para solucionar el problema planteado:

- ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información (SGSI)

- ISO/IEC 27002: Código de Buenas prácticas para la gestión de la seguridad de la información
- NIST Cybersecurity Framework (CSF)
- CIS Controls (Center for Internet Security)
- OWASP (Open Web Applications Security Project)
- GDPR (Reglamento General de Protección de Datos)
- ITIL (Information Technology Infraestructure Library)

Análisis de benchmarking de herramientas de software y hardware aplicables

Se estará realizando un análisis de las herramientas tecnológicas existentes en el mercado y que permiten la automatización de procesos de detección y corrección de vulnerabilidades:

- Herramientas de detección de vulnerabilidades: Nessus, OpenVas, Qualys, etc.
- Herramientas de automatización para corrección de vulnerabilidades: Ansible, Puppet, Chef
- Herramientas de Gestión de Incidentes y respuestas a incidentes: Servicenow, Splunk
- Herramientas de monitoreo: SOAR, SEM
- Firewalls de nueva generación
- IDPS-IPS
- Soluciones de EndPoint

Estas herramientas podrán compararse con las que actualmente se utilizan en el INS y de esta forma establecer parámetros de comparación.

CAPÍTULO 4: ANALISIS DE RESULTADOS

En este capítulo se presentan y analizan los resultados obtenidos a partir de la implementación de los métodos y técnicas descritos en el marco metodológico. El propósito de este análisis es validar el cumplimiento de los objetivos planteados en esta investigación y proporcionar una visión clara sobre el impacto de las propuestas desarrolladas.

Se parte de los datos recolectados mediante las herramientas e instrumentos definidos, los cuales han sido procesados y organizados para facilitar su interpretación. El enfoque principal radica en examinar cómo las variables estudiadas se relacionan con la problemática inicial, permitiendo identificar patrones, tendencias y áreas de mejora en la gestión de detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS).

A lo largo de este capítulo, se exponen los resultados en función de cada objetivo específico, detectando hallazgos clave que fundamentan la propuesta del modelo automatizado. Además, se incluye un análisis crítico que compara los resultados obtenidos con los estándares internacionales y las mejores prácticas en ciberseguridad, con el fin de garantizar la aplicabilidad y relevancia del modelo planteado.

El análisis no solo busca confirmar los beneficios de las herramientas y metodologías seleccionadas, sino también identificar posibles limitaciones o áreas que requieran ajustes en futuras investigaciones.

El capítulo también incluye el correspondiente estudio de factibilidad completo y el respectivo análisis de riesgos del proyecto.

Definición del tamaño de la muestra

Para obtener la muestra se aplicó la fórmula definida en el capítulo 3, de acuerdo con los resultados obtenidos el tamaño de esta es el siguiente:

Fórmula: Z2 * (p) * (1-p) / c2

Tamaño de muestra: 15

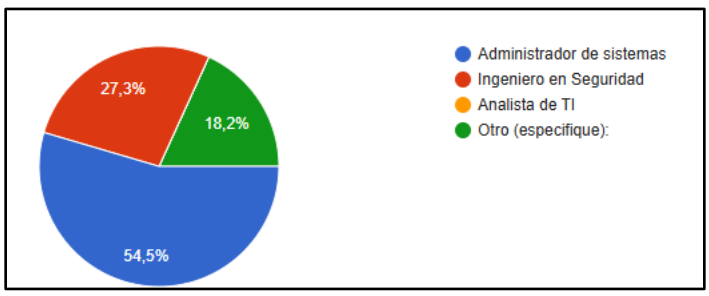
Resultado de encuestas

Se realizó una encuesta “Encuesta #1” (Anexo #1) sobre la población meta obteniendo los siguientes resultados:

Pregunta 1. Ante la consulta ¿Cuál es su rol dentro de la organización? Los resultados fueron los siguientes, observados en la figura 16.

Figura 16

Resultados Pregunta #1 Encuesta INS

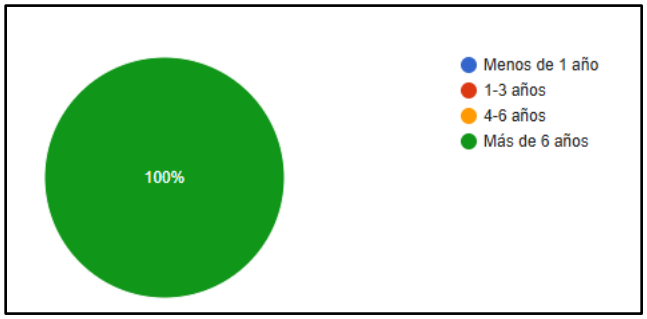


De acuerdo con estos datos, el 54,5 % de los encuestados son funcionarios que administran los sistemas y la infraestructura del INS quienes serán los encargados de implementar la automatización en el nivel en el que esta se vaya a implementar , un 27,3 % son Ingenieros en la parte de seguridad de TI quienes se encargan de gestionar el proceso de detección y corrección de vulnerabilidades, mientras que el 18,2 % forman parte de otras áreas importantes de TI involucradas en este proceso (redes, telecomunicaciones, etc.).

Pregunta 2. Ante la consulta ¿Cuántos años de experiencia en el área de TI? Los resultados fueron los siguientes, observados en la figura 17:

Figura 17

Resultados pregunta #2

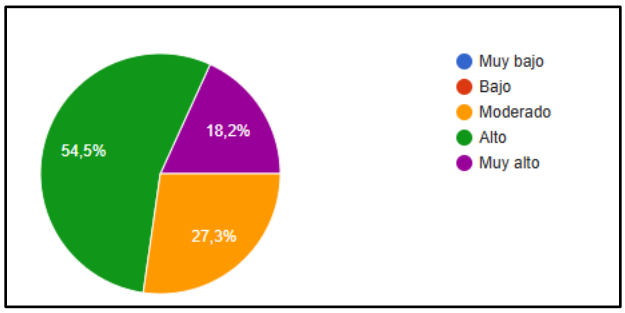


Como se puede observar, el 100 % de los encuestados tienen más de 6 años de experiencia en el área de TI, esto indica que las respuestas y criterios obtenidas son totalmente calificados y que existe personal ampliamente capacitado y experimentado que favorece la implementación de la automatización.

Pregunta 3. Ante la consulta: En escala del 1 al 5, evalúe su conocimiento sobre las vulnerabilidades más comunes en la infraestructura tecnológica, los resultados fueron los siguientes, observados en la figura 18:

Figura 18

Resultados pregunta #3

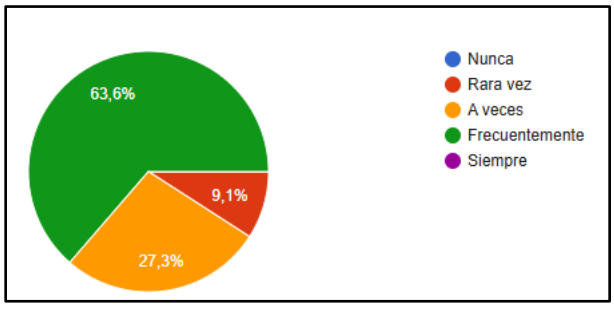


Esto indica que un 54,5 % de los encuestados está al tanto de las vulnerabilidades más comunes que se presentan en la infraestructura del INS, esto permite tener un alto grado de concientización al respecto y de disposición a las soluciones que se puedan presentar y proponer, el 27,3 % de los encuestados tiene un conocimiento moderado de las vulnerabilidades presentadas y un 18,2 % tiene un conocimiento muy alto de esta problemática, es importante destacar que este porcentajes es relativamente bajo y se debe trabajar en aumentarlo.

Pregunta 4. Ante la consulta ¿Con qué frecuencia detecta vulnerabilidades críticas en la infraestructura del INS?, los resultados obtenidos se muestran en la figura 19:

Figura 19

Resultados pregunta 4



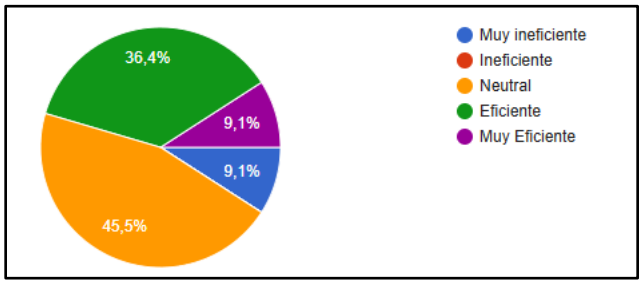
Estos resultados muestran que la detección de vulnerabilidades es una situación frecuente dentro de la infraestructura del INS esto lo demuestra el 63,6 % de resultados, también

determinado porque una gran parte de la población encuestada forma parte del equipo Chirripó que tiene como parte de sus funciones la corrección de las vulnerabilidades que son detectadas por el área de Seguridad de TI. Un 27,3 % indica que a veces detecta vulnerabilidades y un 9,1 % indica que rara vez, esto a su vez, tiene que ver con las funciones de cada uno de estos funcionarios. El aporte positivo de este resultado a la investigación se basa en que con la automatización se espera que este porcentaje disminuya de forma considerable.

Pregunta 5. Ante la consulta: En escala del 1 al 5 ¿cómo evaluaría la eficiencia del proceso actual de detección de vulnerabilidades?, los resultados fueron los siguientes como se observa en la figura 20:

Figura 20

Resultados pregunta #5

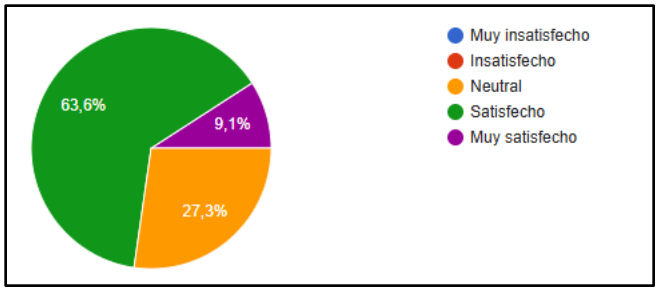


El resultado Neutral de un 45,5 % deja saber que existen aún muchos puntos de mejora en el proceso actual, con el fin de aumentar esa puntuación, un porcentaje importante 36,4 % lo ve como eficiente, mientras que existen porcentajes iguales en Muy ineficiente y Eficiente, esto claramente puede verse afectado por el rol que tiene cada uno de los ingenieros encuestados. Dados estos resultados se determina que la aplicación de una metodología ágil para la automatización de procesos es requerida y aportará al proceso.

Pregunta 6. Ante la consulta ¿Qué tan satisfecho está con la herramienta actual utilizada para la detección de vulnerabilidades?, los resultados obtenidos se muestran en la siguiente figura 21:

Figura 21

Resultados pregunta #6

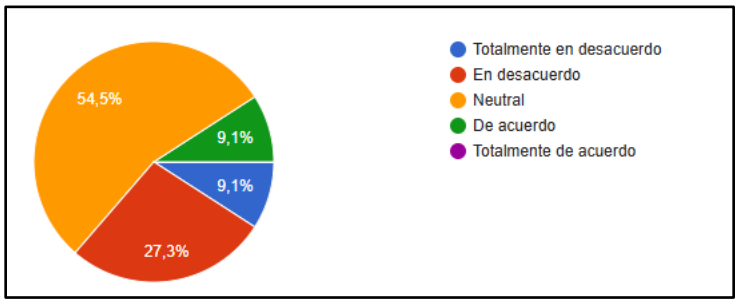


Se observa que ampliamente se tiene un alto nivel de satisfacción 63,6 % con el uso de la herramienta actual (Nessus), por lo tanto, se puede concluir que brinda un servicio eficiente y esperado, interesante notar que hay un 27,3 % de respuestas neutrales probablemente provocado por el desconocimiento de la herramienta y su uso, así como un 9.1 % Muy Satisfecho. Esto indica que la automatización del proceso debe enfocarse en otra dirección, pues la parte de detección y escaneo de la infraestructura está siendo realizada de forma adecuada por la herramienta Nessus.

Pregunta 7. Ante la consulta ¿El tiempo promedio de corrección de vulnerabilidades es adecuado?, los resultados se muestran en la figura 22:

Figura 22

Resultados pregunta #7

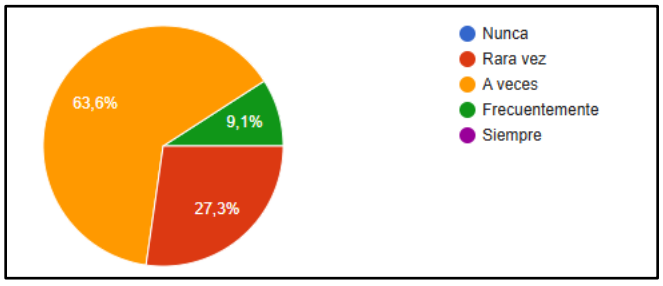


Es importante destacar que el porcentaje mayor del 54,5 %, y que corresponde a respuestas Neutrales, debe ser muy tomado en cuenta, pues esto puede depender de varios factores, sin embargo, en la corrección de vulnerabilidades el tiempo es uno de los factores principales a tomar en cuenta, de igual forma el segundo valor más respondido un 27,3 % que corresponde a En desacuerdo debe llamar la atención, y analizar en detalle a que se deben dichas respuestas. La automatización de algunos de los procesos que forman parte de la corrección de vulnerabilidades tiene como otro de sus objetivos mejorar estos tiempos de forma sustancial.

Pregunta 8. Ante la consulta ¿Qué tan frecuentemente el proceso manual de detección y corrección de vulnerabilidades presenta errores?, los resultados se muestran en la figura 23:

Figura 23

Resultados pregunta #8



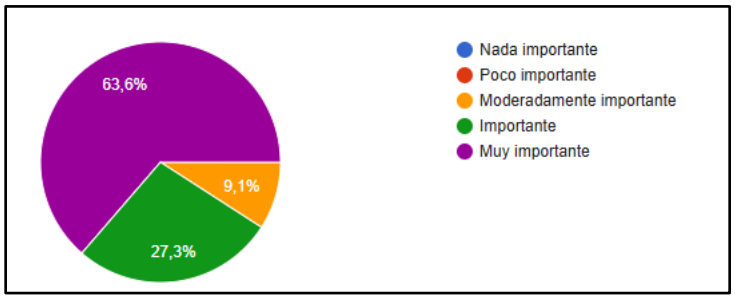
Al igual que en la pregunta anterior el resultado mayoritario que es de un 63,6 % y que indica A veces, debe llamar la atención y determinar qué tan seguido y los tipos de fallas que

presenta el proceso, pues esto es básico para mejorarlo y perfeccionarlo cada vez más. Con la implementación de automatización en algunos de los procesos, se busca reducir el error en las tareas, principalmente el error humano.

Pregunta 9. Ante la consulta: En una escala del 1 al 5, ¿qué tan importante considera la automatización para mejorar la seguridad de la infraestructura tecnológica?, los resultados se muestran en la figura 24:

Figura 24

Resultados pregunta #9

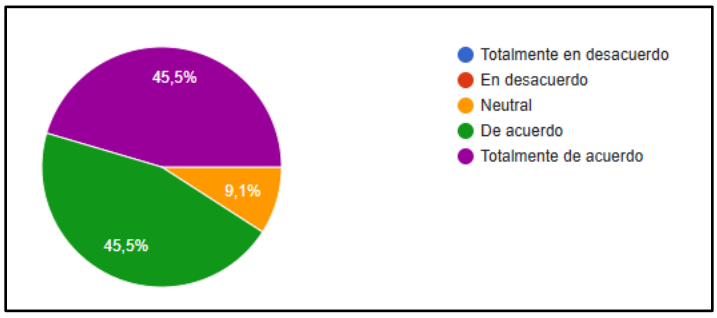


Se concluye que existe una amplia necesidad y disposición de parte de la parte técnica en implementar la automatización en la detección y corrección de vulnerabilidades, el 63,6 % de los encuestados se muestran a favor y ven como muy importante realizar esta transición a la automatización o al menos implementarla como un complemento a lo ya existente.

Pregunta 10. Ante la consulta ¿Cree que la automatización reducirá el tiempo promedio de corrección de vulnerabilidades?, los resultados se muestran en la figura 25:

Figura 25

Resultados pregunta #10

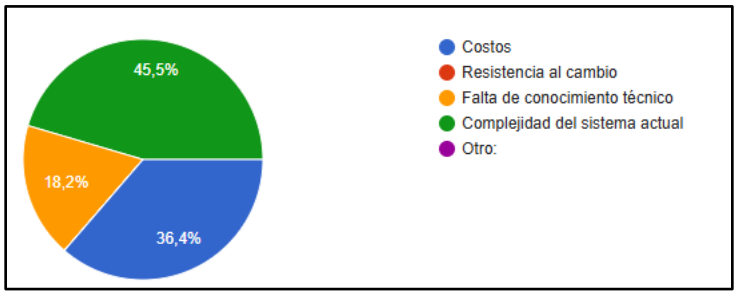


Existe mucha expectativa de que la automatización de estos procesos va a ayudar en la reducción de tiempos promedios de corrección de vulnerabilidades, los encuestados estuvieron de acuerdo y totalmente de acuerdo en un 45,5 %, para un total de un 91 % general por lo que una vez más se detecta que existe mucha apertura a la implementación de automatización.

Pregunta 11. Ante la consulta ¿Qué barreras considera que podrían dificultar la implementación de un sistema automatizado?, los resultados se muestran en la figura 26:

Figura 26

Resultados pregunta #11



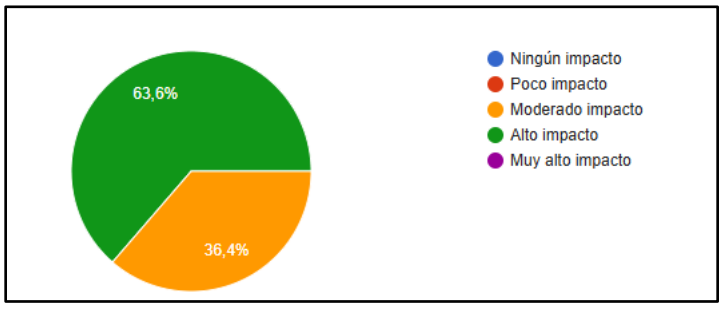
En este caso, un 45,5 % de los encuestados indicaron la complejidad del sistema actual como el principal factor que presentaría una barrera en la implementación, los costos también son vistos como una de las principales barreras con un 36,4 %, esto hace que las herramientas propias a las cuales se tenga acceso directo e inmediato tomen más fuerza para reforzar la

automatización en algunos procesos que colaboren en los procesos de detección y corrección de vulnerabilidades, en un menor porcentaje 18,2 % se menciona la falta de conocimiento técnico como otro de los factores, sin embargo, en este caso la capacitación jugaría un papel importante.

Pregunta 12. Ante la consulta ¿Qué impacto cree que tendría la automatización en la reducción de errores humanos?, los resultados se muestran en la figura 27:

Figura 27

Resultados pregunta #12

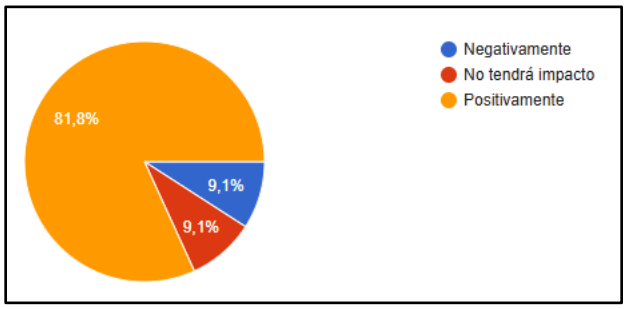


Como es de esperarse uno de los objetivos de la automatización es precisamente tratar de eliminar o minimizar los errores humanos que se presentan en los procesos, de ahí que es esperable el resultado del 63,6 %.

Pregunta 13. Ante la consulta: En su opinión ¿Cómo afectaría la automatización al cumplimiento de normativas de seguridad (ejemplo: ISO 27001) ?, los resultados se muestran en la figura 28:

Figura 28

Resultados pregunta #13

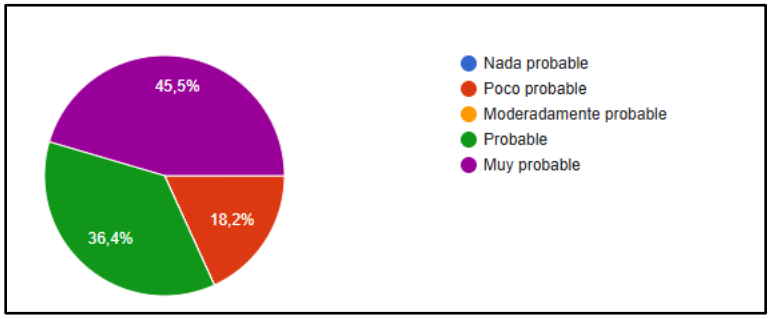


Claramente las respuestas son positivas en un 81,8 %, está claro que la automatización ayudaría a la organización en el cumplimiento de las normas internacionales.

Pregunta 14. Ante la consulta ¿Qué tan probable es que la automatización aumente la capacidad de respuesta ante incidentes de seguridad?, los resultados se observan en la figura 29:

Figura 29

Resultados pregunta #14

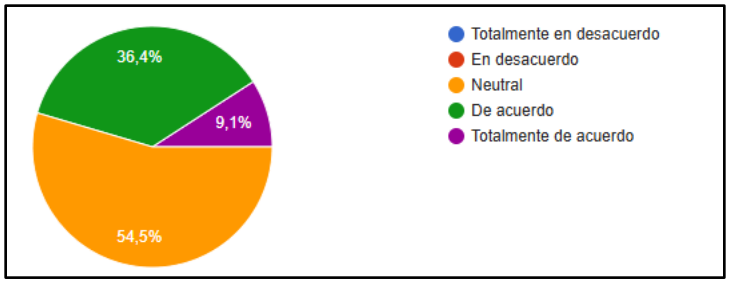


Nuevamente se nota opiniones favorables en el entorno de los ingenieros encuestados, siendo que la opción de que sea muy probable que la automatización aumente la capacidad de respuestas es la mayor con un 45,5 % y probable tiene un 36,4 %. El contar con la aprobación y disposición de los ingenieros involucrados en el proceso es muy importante, ya que esto facilitará la implementación sugerida en esta investigación.

Pregunta 15. Ante la pregunta ¿El personal actual tiene el conocimiento necesario para manejar sistemas automatizados de detección y corrección?, el resultado se muestra en la figura 30:

Figura 30

Resultados pregunta #15

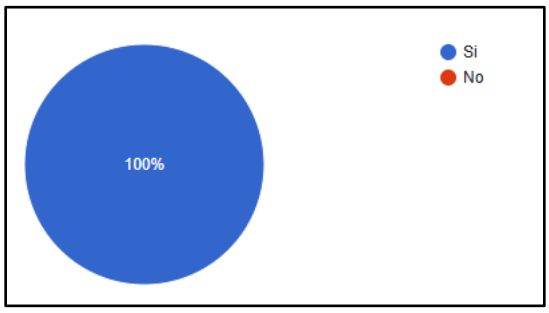


Si bien es cierto el resultado principal de un 54,5 % es neutral, también es cierto que el personal como se vio en una de las respuestas anteriores es personal con mucha experiencia y que puede adaptarse rápidamente a nuevas tecnologías, gestionando la capacitación necesaria y respectiva.

Pregunta 16. Ante la pregunta ¿Considera que es necesaria una capacitación para implementar un sistema automatizado?, los resultados se muestran en la figura 31:

Figura 31

Resultados pregunta #16

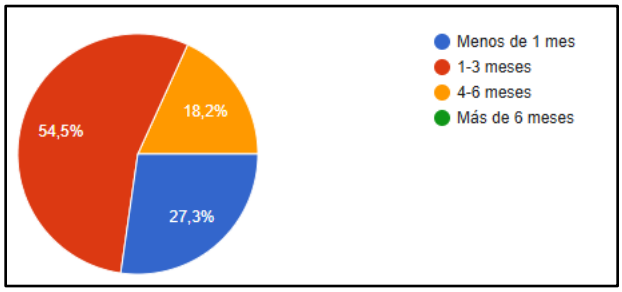


En este caso el resultado es contundente y además necesaria la capacitación en cualquier implementación de una nueva tecnología.

Pregunta 17. Ante la consulta ¿Cuánto tiempo cree que debería durar una capacitación sobre el nuevo sistema automatizado?, los resultados se muestran en la figura 32:

Figura 32

Resultados pregunta #17

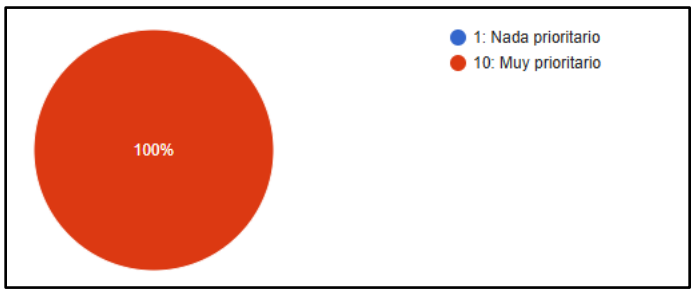


Tomando en cuenta que es una política institucional el buscar capacitaciones con certificaciones incluidas, de ahí se desprende que el resultado mayoritario sea de 1 a 3 meses como mínimo, esto con un 54,5 %, pues este es el tiempo ideal para capacitarse adecuadamente, unido al uso que se haga de la o las herramientas.

Pregunta 18. Ante la consulta: En una escala de 1 al 10, ¿qué tan prioritario considera que es implementar la automatización en el INS?, los resultados se muestran en la figura 33:

Figura 33

Resultados pregunta #18

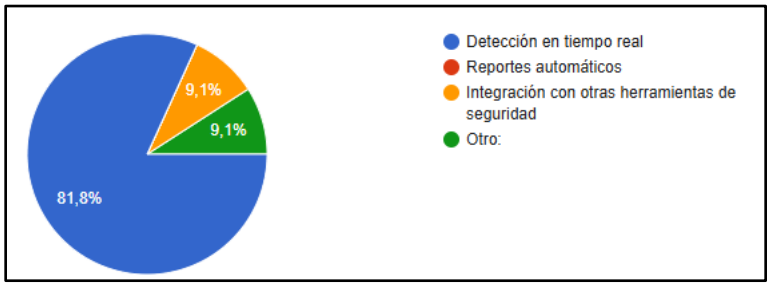


En este caso el resultado es contundente con respecto a la prioridad que tiene desde el punto de vista de la parte técnica la implementación de automatización en el INS.

Pregunta 19. Ante la consulta: En su opinión, ¿qué funcionalidad es más importante en un sistema automatizado?, los resultados están en la figura 34:

Figura 34

Resultados pregunta #19

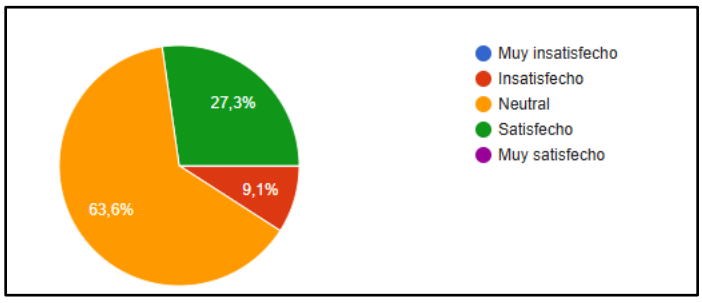


Se concluye de estas respuestas que la detección en tiempo real es uno de los factores más importantes y que son más solicitados por los ingenieros el 81,8 % indica claramente la importancia de potenciar la herramienta de escaneo actúal (Nessus) y explorar si existen opciones en dicha herramienta que permitan esta inmediatez.

Pregunta 21. Ante la consulta ¿Qué tan satisfecho está con la integración actual de herramientas de detección de vulnerabilidades con otras plataformas de seguridad?, los resultados se muestran en la figura 35:

Figura 35

Resultados pregunta #21



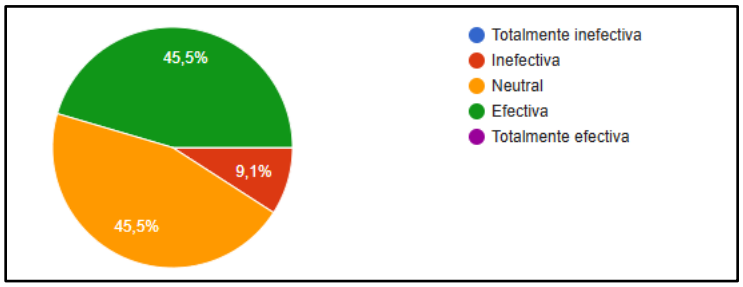
Debido a que no existen actualmente desarrollos importantes en este sentido la respuesta predominante con un 63,6 % es la neutral, sin embargo, con las integraciones existentes se

muestra un 27,3 % de satisfacción lo cual es bastante importante. La intención de este proyecto es que con la automatización de procesos asociados a las labores de detección y corrección de vulnerabilidades se logre potenciar el 63 % obtenido y convertirlo en una visión y opinión favorables en este sentido.

Pregunta 22. Ante la consulta ¿Qué tan efectiva considera la priorización de vulnerabilidades críticas en el proceso actual?, los resultados se muestran en la figura 36:

Figura 36

Respuestas pregunta #22

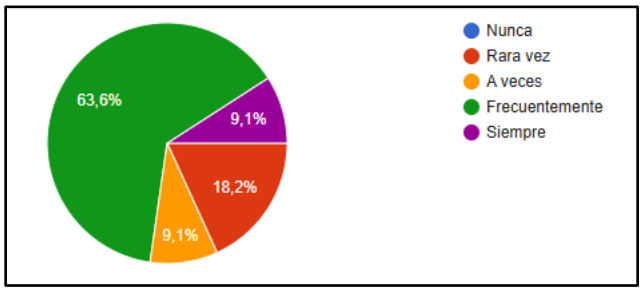


En este caso hay una opinión divida en cuanto a que dicha priorización haya sido efectiva, pues un 45,5 % considera que lo es, mientras que un porcentaje igual lo considera neutral, esto indica que se debe hacer una revisión de esta priorización y ver si se deben realizar cambios. Es importante destacar en este caso que la priorización de las vulnerabilidades viene también definida desde la Dirección del departamento, basándose en varios aspectos como la criticidad de los sistemas alojados en los servidores respectivos, en este sentido es muy importante contar con la participación directa de las jefaturas y en consenso con el negocio y los ingenieros responsables del proceso definir de una mejor forma dichas prioridades.

Pregunta 23. Ante la consulta: En su experiencia, ¿con qué frecuencia los equipos de TI logran corregir vulnerabilidades antes de que se conviertan en incidentes?, los resultados se muestran en la figura 37:

Figura 37

Respuestas a la pregunta #23

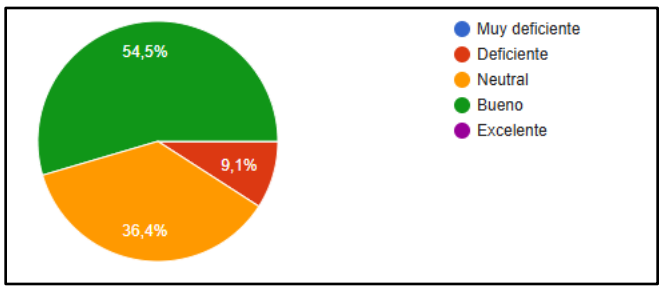


De acuerdo con este resultado, se presentan opiniones favorables respecto a la corrección adecuada de las vulnerabilidades, esto lo demuestra el 63,6 % que brindaron la opinión de que es frecuente. Se debe estudiar los casos de los diferentes porcentajes y validar si en esos casos específicos la automatización viene a brindar una solución definitiva para que se obtenga un 100 % de frecuencia en este sentido.

Pregunta 24. Ante la consulta ¿Cómo describiría el nivel de cooperación entre los equipos responsables de detectar y corregir vulnerabilidades?, los resultados se muestran en la figura 38:

Figura 38

Respuestas de la pregunta #24



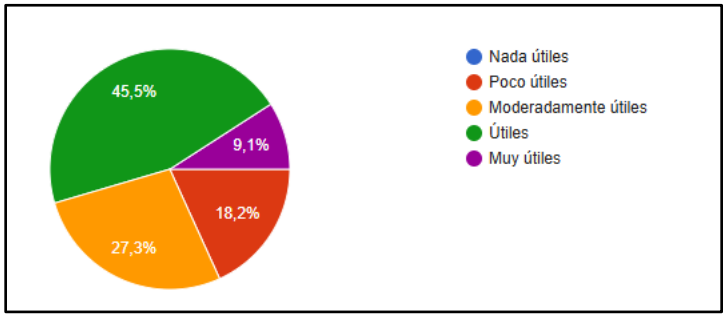
En términos generales el nivel de cooperación es bueno, esto lo demuestra el 54,5 %, tomando en cuenta que esta es una labor en la que deben participar todas las áreas de TI y de la organización con el fin de garantizar el éxito en estas labores. Las labores de automatización propuestas en este proyecto Se debe brindar más capacitación a distintas áreas, mejorar los

contratos con empresas externas que brindan servicios y por supuesto automatizar la mayor cantidad de procesos.

Respuesta 25. Ante la consulta ¿Qué tan útiles son los reportes actuales de vulnerabilidades para la toma de decisiones?, los resultados se muestran en la figura 39:

Figura 39

Respuestas a pregunta #25

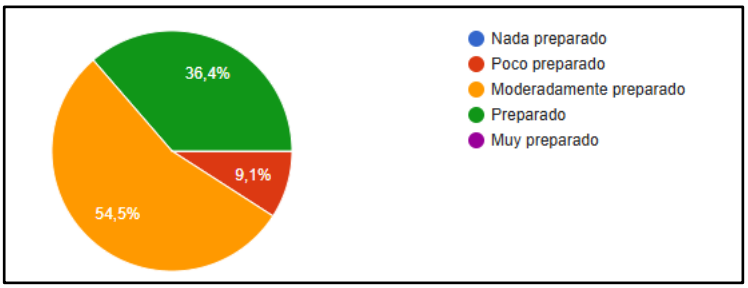


Este es un factor importante para tomar en cuenta, pues los reportes generados por la herramienta Nessus son los que se toman como base para realizar la corrección de vulnerabilidades, de tal forma que el porcentaje 45,5 % que los califica como útiles debería tratar de ampliarse. Además, se debe ahondar en los motivos de quienes lo calificaron con un 27,3 % como moderadamente útiles, valorar herramientas adicionales con más funcionalidades y potenciar el Nessus en lo máximo posible, si es preciso buscar capacitaciones adicionales de la herramienta.

Pregunta 26. Ante la consulta: en una escala del 1 al 5, ¿qué tan preparado cree que está el INS para adoptar nuevas tecnologías de automatización en seguridad?, las respuestas se muestran en la figura 40:

Figura 40

Resultados pregunta #26

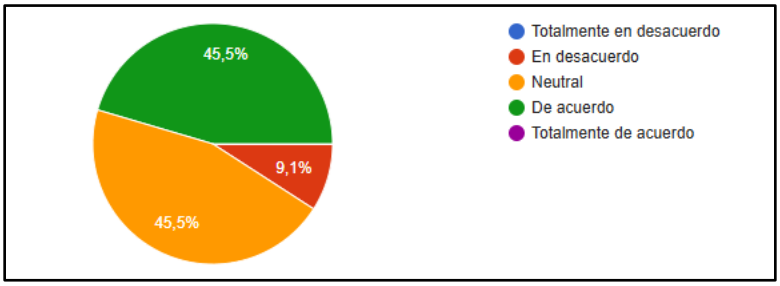


De acuerdo con los ingenieros consultados la mayor parte un 54,5 % respondió que el INS se encuentra moderadamente preparado para la adopción de nuevas tecnologías, un 36,4 % indica que el INS está preparado, lo importante acá es notar que se han realizado varios cambios tecnológicos a través de los años que se han podido implementar con éxito por lo que este tipo de cambios pueden realizarse sin problemas.

Pregunta 27. Ante la consulta ¿Considera que la automatización del proceso permitirá ahorrar recursos económicos en comparación con los métodos manuales?, las respuestas se muestran en la figura 41:

Figura 41

Respuestas a la pregunta #27



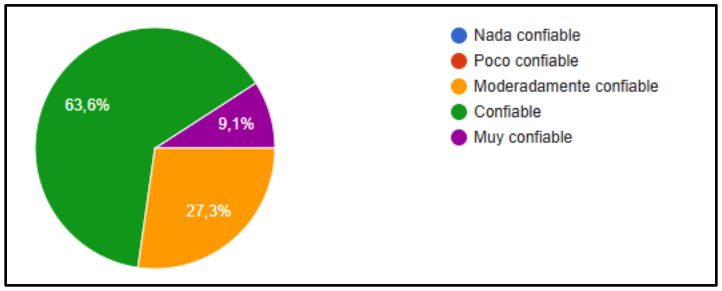
Existe en este caso una tendencia a pensar que si bien es cierto se puede ahorrar en recursos 45,5 %, un porcentaje igual se mantiene de forma neutra, es decir con algunas reservas al respecto, mientras que un 9,1 % no cree que esto vaya a representar un ahorro de recursos. En

un caso específico se puede valorar como la automatización del proceso de aplicación de parches en los servidores de la plataforma Windows que es un proceso íntimamente ligado a la corrección de vulnerabilidades, pasaría a tener un ahorro en el rubro de pago de horas extras de casi un 400 %, pues de tener 5 funcionarios en un fin de semana aplicando los parches, se pasaría a solamente una persona verificando su aplicación y cualquier posible error que el proceso pueda generar y corregir. La posibilidad de disminuir problemas e interrupciones de los sistemas que normalmente representan para la organización pérdidas económicas representa otro factor importante de ahorro de recursos económicos.

Pregunta 28. Ante la consulta ¿Qué tan confiable cree que será el sistema automatizado para la detección de nuevas vulnerabilidades en comparación con los sistemas manuales?, las respuestas se muestran en la figura 42:

Figura 42

Respuestas a la pregunta #28

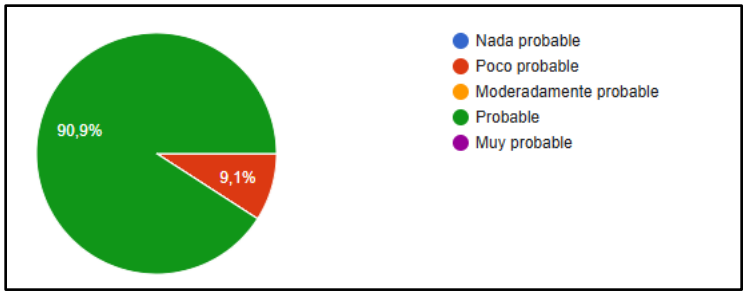


Basado en estas respuestas se puede definir que existe confianza en que un sistema automatizado o la automatización de algunos de los procesos existentes puede generar resultados confiables a diferencia de sistemas más manuales, esto lo demuestra el 63,6 % de las respuestas en este sentido.

Pregunta 29. Ante la consulta ¿Qué tan probable es que la automatización impulse cambios positivos en la cultura organizacional del INS respecto a la seguridad de TI?, los resultados se muestran en la figura 43:

Figura 43

Resultados pregunta #29



Cómo se puede observar en los resultados, ampliamente un 90,9 % de los encuestados ve de forma positiva y probable que la automatización de procesos brinde cambios positivos en la cultura organizacional del INS.

Resultado de entrevistas

Se realizaron dos entrevistas con el propósito de comprender las percepciones y experiencias de los entrevistados con respecto al tema de la automatización de procesos para la detección y corrección de vulnerabilidades en infraestructura tecnológica, además de entender el grado de satisfacción con el proceso actual y las mejoras que puede representar la automatización tanto en la cantidad de incidentes atendidos como en la calidad de la atención y la mejora que puede representar en tiempos y en fallas humanas entre otros aspectos.

Los entrevistados fueron el jefe de la Unidad de Seguridad de TI, así como el director del Departamento de Tecnologías de la Información, ambas figuras claves en la toma de decisiones del proceso de atención de vulnerabilidades.

En primera instancia se le consultó al encargado de Seguridad de TI sobre los siguientes tópicos y estas fueron las respuestas emitidas:

"¿Cuál es su visión general sobre el estado actual de la seguridad tecnológica del INS?

En general considerando la escala de 1 a 10, donde 1 es el más bajo y 10 el más alto, diría objetivamente que 7"

"¿Cómo se alinean las políticas de seguridad actuales con los procesos de detección y corrección de vulnerabilidades?

La poltica de ciberseguridad dicta que debe existir un proceso de cierre de brechas, el cual se instauro a nivel tecnico, a partir del 2021, esto en conjunto con análisis de vulnerabilidades constantes."

"Desde su perspectiva, ¿qué tan efectivo es el proceso actual para gestionar vulnerabilidades críticas?

No es el mejor, por la limitada capacidad instalada y también conocimiento, sin embargo, el esfuerzo si se realiza."

"¿Qué brechas en la seguridad identifica en el proceso manual actual?

Procesos manuales no se ejecutan por ser poco eficiente el mismo, todo es mediante herramienta especializada."

"¿Cómo cree que la automatización del proceso contribuirá a mitigar riesgos de seguridad?

El proceso de identificación esta automatizado, el proceso de cierre de brechas si es manual, la automatización en empresas con sistemas legados no es una sana practica pues puede dejar aplicaciones fuera de línea al intentar corregir una vulnerabilidad, debe ser manual bajo este escenario."

"¿Qué impacto tendrá la automatización en el cumplimiento de normativas como ISO 27001 o el marco NIST?

Si se llegase a ese entorno, agilizaría la solución de brechas, lo cual es recomendado principalmente por NIST."

"¿Qué controles considera esenciales para asegurar la efectividad del sistema automatizado?

Ingreso de alertas con la debida categorización, considerando siempre de más a menos, es decir, de las críticas a las bajas, la exposición se reduciría drásticamente, que se puedan contar con inicio, fin y resultado obtenido."

"¿Cómo planea medir y gestionar los riesgos asociados a la implementación de la automatización?

El riesgo es un resultado de la incertidumbre del cumplimiento de los objetivos empresariales, bajo esa perspectiva, la metodología de riesgos aplicada implica la medición objetiva de los mismos mediante varios instrumentos, para el caso aplicaría valora si esa automatización cumple con ese objetivo de la política de seguridad y los objetivos empresariales."

"¿Qué tan preparada está la organización para adoptar cambios relacionados con la automatización?

Todo cambio implica resistencia, la cultura organizacional actual es bastante reacia a cambios, se necesitaría una culturización y concientización importante, mostrando los beneficios de lo que implica la automatización de tareas y que estas no ponen en riesgo el puesto laboral."

"¿Qué medidas sugiere para promover una cultura de seguridad que respalde el uso de herramientas automatizadas?

el eslabón más débil de la cadena de ciberseguridad es el usuario final, viéndolo de forma positiva, el usuario es el primer control para evitar ciberataques, desde esa perspectiva se trabajaria en

culturización del personal, técnico y no técnico sobre los beneficios de la automatización de tareas.”

“¿Qué métricas utilizará para evaluar el éxito de la automatización en términos de seguridad?

Resultados obtenidos, cantidad de vulnerabilidades de categoría importante detectadas vs cantidad cerrada o atendida y en qué periodo de tiempo, así mismo, tiempo invertido en cada uno como éxito o falla de los sistemas tratados.”

“¿Qué desafíos estratégicos anticipa durante y después de la implementación?

Principalmente la resistencia al cambio, inventario de activos actualizado, y mantenimiento en el tiempo, lo que se corrige hoy mañana ya puede contar con otra brecha que debe ser atendida.”

“Desde su perspectiva como Encargado de Seguridad de TI, ¿qué factores son clave para una implementación exitosa?

Compromiso del personal, herramientas adecuadas, delegación de actividades, culturización, especialización y capacitación.”

“¿Qué consejos le daría al equipo técnico y a la alta gerencia para garantizar el éxito del proyecto?

Dar las herramientas necesarias, el espacio necesario, pero sobre todo comprender la siguiete frase: "Si piensas que la tecnología puede resolver tus problemas de seguridad, entonces es que no entiendes los problemas y no entiendes la tecnología" Bruce Schneier" “

Análisis

De las anteriores respuestas se observa que existe claramente una visión objetiva del proceso actual, el cual es calificado con un 7 en escala del 1 al 10, esto indica que aún hay aspectos en los cuales se debe mejorar, existe un proceso ya maduro instaurado hace casi 4 años,

sin embargo, es un proceso manual en todas sus facetas, con excepción del escaneo que se realiza sobre la plataforma, que, a pesar de esto, no deja de ser un proceso administrado por personas.

Existe además una clara conciencia de que el proceso actual no es el mejor, sin embargo si se plantea el reto de automatizar el proceso completo, pues de acuerdo con el entrevistado sobre todo la parte de la corrección de vulnerabilidades en empresas con sistemas legados no es recomendable, ya que se pueden presentar interrupciones de sistemas al momento de realizar dichas correcciones, de ahí que se plantea en esta investigación la automatización de procesos específicos que están íntimamente ligados al proceso, por ejemplo el parchado de servidores.

En las respuestas además se brindan importantes detalles a tomar en cuenta a la hora de hacer la propuesta de automatización que pretende realizar esta investigación, en cuanto a prioridades, gestión de riesgos, aplicación de normas, etc.

Además, se detallan aspectos importantes en cuanto a la organización como tal, aspectos de la preparación que existe para afrontar cambios tecnológicos que impliquen automatización, así como aspectos propios de la cultura organizacional en los cuales se debe trabajar aun más de lo que se ha trabajado hasta el día de hoy.

La segunda entrevista fue realizada al director de TI, máximo jerarca dentro de la organización en aspectos de tecnología, a continuación, se detallan las consultas hechas y sus respectivas respuestas:

“¿Cuál es su rol principal en la gestión de la infraestructura tecnológica del INS?

Soy el jefe de la Dirección de Tecnologías de Información del Instituto Nacional de Seguros, encargado de gestionar los recursos técnicos, tecnológicos y humanos de esta dependencia y de brindar resultados a la Gerencia de la Institución.”

“¿Cómo se involucra su equipo en la detección y corrección de vulnerabilidades?

Actualmente tenemos varios frentes en ese sentido tanto desde la parte de seguridad tecnológica como de los equipos, cada una de las áreas debe tomar las medidas respectivas tanto en hardware como software, además contamos con el grupo Chirripó que se encarga directamente de la atención de vulnerabilidades."

"¿Qué herramientas utilizan actualmente para la detección de vulnerabilidades?

Actualmente se utiliza la herramienta Nessus para el escaneo de la infraestructura."

"¿Cuál es el tiempo promedio que toma identificar y corregir una vulnerabilidad crítica?

Depende de varios factores, la identificación se realiza por medio de los escaneos mensuales, la corrección depende del sistema involucrado y el tipo de trabajo que se deba hacer para corregir, pero normalmente se toma en promedio 15 días."

"¿Cuáles son las principales limitaciones del proceso manual en términos de eficiencia y precisión?

Principalmente el problema con el proceso manual es que siempre está presente la posibilidad del error humano, esto puede generar problemas adicionales, en cuanto a tiempo y servicios."

"En su opinión, ¿cómo podría la automatización mejorar los tiempos de respuesta ante vulnerabilidades?

El automatizar los procesos cuando se logra establecer y madurar el proceso, es una gran ventaja en muchos casos la corrección puede ser casi inmediata y esto representaría una gran ventaja en cuanto a las mejoras en los tiempos de respuesta."

"¿Qué aspectos técnicos considera más desafiantes en la implementación de un sistema automatizado?

El aprendizaje y manejo de la o las herramientas de parte de nuestros técnicos."

"¿Cómo afectará la automatización a la carga de trabajo de su equipo?

Esperaría que afecte de una forma positiva, recordemos que los funcionarios que forman parte del equipo Chirripó, no se dedican a esto al 100 %, sino que tienen otras funciones y realizan sus funciones normales y solo dedican cierta cantidad de horas a la semana a las vulnerabilidades, por lo tanto, se esperaría que la automatización de procesos tenga un impacto positivo en estas cargas."

"¿La infraestructura actual del INS está preparada para integrar un sistema automatizado?

Creemos que sí estamos preparados para una integración de este tipo."

"¿Qué integraciones considera esenciales entre el sistema automatizado y las herramientas actuales de monitoreo o gestión?

La importancia principal es la integración de los datos en tiempo real, de tal forma que se cuenta con datos precisos y exactos en el momento, esto representa una gran ventaja para los equipos de monitoreo y atención de incidencias."

"¿Qué riesgos o desafíos de seguridad percibe al automatizar este proceso?

Me parece que los normales en toda implementación y automatización de un proceso, se debe contar con los aspectos principales de seguridad, validaciones adecuadas, accesos adecuados, monitoreo constante del funcionamiento de la herramienta."

"¿Cómo garantizar que el sistema automatizado sea confiable y se mantenga actualizado frente a nuevas vulnerabilidades?

Esto sería parte del estudio previo que se debe hacer antes de adquirir algún software, se debe establecer un filtro adecuado con los parámetros necesarios y establecidos por nuestro departamento de seguridad para que cumplan con todos los requisitos respectivos."

"¿El personal de TI tiene el conocimiento técnico necesario para gestionar una herramienta automatizada?

Nuestro personal es altamente capacitado y experimentado en el manejo de nuevas herramientas, por lo tanto, creo que no tendrían problema en adaptarse y aprender de estas nuevas tecnologías."

"¿Qué tipo de capacitación o recursos considera necesarios para una implementación exitosa?

Normalmente buscamos que se nos brinden certificaciones con el fin de cumplir a cabalidad con el desarrollo de nuestros funcionarios."

"¿Qué beneficios estratégicos cree que podría aportar la automatización al INS en términos de seguridad y eficiencia?

Aportaría en la optimización de la atención, en reducir el error humano, en integrar las diferentes plataformas."

"¿Qué recomendaciones daría para asegurar una transición exitosa hacia la automatización?

Que se realicen los estudios de forma detallada, se generen los laboratorios y las pruebas del caso, y se cumpla con los tiempos adecuados de cronograma."

Análisis

De las respuestas obtenidas, existe una gran apertura a la automatización de procesos, eso sí, esta debe realizarse de una forma gradual y que principalmente no represente un riesgo para la organización en cuanto a posibilidad de pérdidas o interrupciones de servicios esenciales. En términos generales se ve la automatización de procesos como algo positivo, que puede impactar directamente en la carga de trabajo de las personas implicadas no solo en el proceso de detección y corrección de vulnerabilidades, sino de otros procesos paralelos que son importantes en la consecución de estos objetivos.

Además, se puede identificar que existe gran seguridad de que tanto la infraestructura actual como el personal están calificados y preparados para asumir el reto de una automatización

de procesos, tomando en cuenta que siempre debe existir el respectivo plan de capacitación y certificación adecuados.

Otro aspecto importante que detalla el director y que es de suma consideración en esta investigación, es el de contar con laboratorios previos a cualquier implementación en producción para garantizar la calidad y eficiencia de la herramienta o herramientas a utilizar.

Análisis de documentación interna

Procedimientos internos de seguridad de TI

De acuerdo con el análisis que se pudo realizar de los procedimientos internos existentes en materia de seguridad en TI, se ha podido extraer el siguiente análisis:

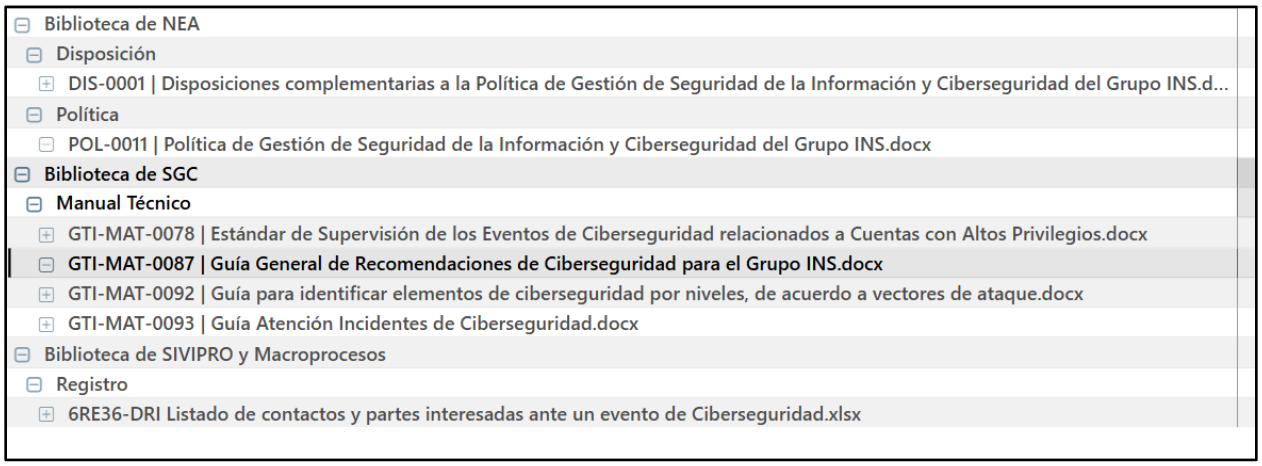
- Existen procedimientos claros establecidos en materia de seguridad informática, que son claramente definidos tanto en el sentido de los usuarios como en el sentido de la infraestructura y aplicaciones.
- Se realizan revisiones periódicas de los procedimientos y se actualizan cuando así se amerite, con el fin de mantenerse actualizados en esta materia.
- Se cumple con la normativa existente en materia de procedimientos internos.

Informes de Auditoría en materia de seguridad informática

De acuerdo con el análisis realizado en cuanto a los informes que se han realizado desde la auditoría interna se han realizado varias publicaciones que se muestran en la siguiente imagen:

Figura 44

Documentación emitida por la Auditoría interna del INS en ciberseguridad



Nota. Fuente (Auditoría Interna INS)

A saber:

- Disposiciones complementarias a la Política de Gestión de Seguridad de la Información y Ciberseguridad del Grupo INS.
- Política de Gestión de Seguridad de la Información y Ciberseguridad del Grupo INS.
- Estándar de Supervisión de los Eventos de Ciberseguridad relacionados a Cuentas con Altos Privilegios.
- Guía General de Recomendaciones de Ciberseguridad para el grupo INS.
- Guía para identificar elementos de ciberseguridad por niveles, de acuerdo a vectores de ataque.
- Guía Atención de Incidentes de Ciberseguridad.
- Listado de contactos y partes interesadas ante un evento de Ciberseguridad.

Políticas internas de seguridad de TI

Existen varias políticas de seguridad informática en este momento activas, se pueden dividir en dos grandes áreas:

- Usuarios: se establecen diferentes políticas a nivel de usuario final, que incluyen entre otros aspectos: cambios de clave mensuales, múltiple factor de autenticación, bloqueos de dispositivos USB, políticas de acceso a aplicaciones, por mencionar algunas.

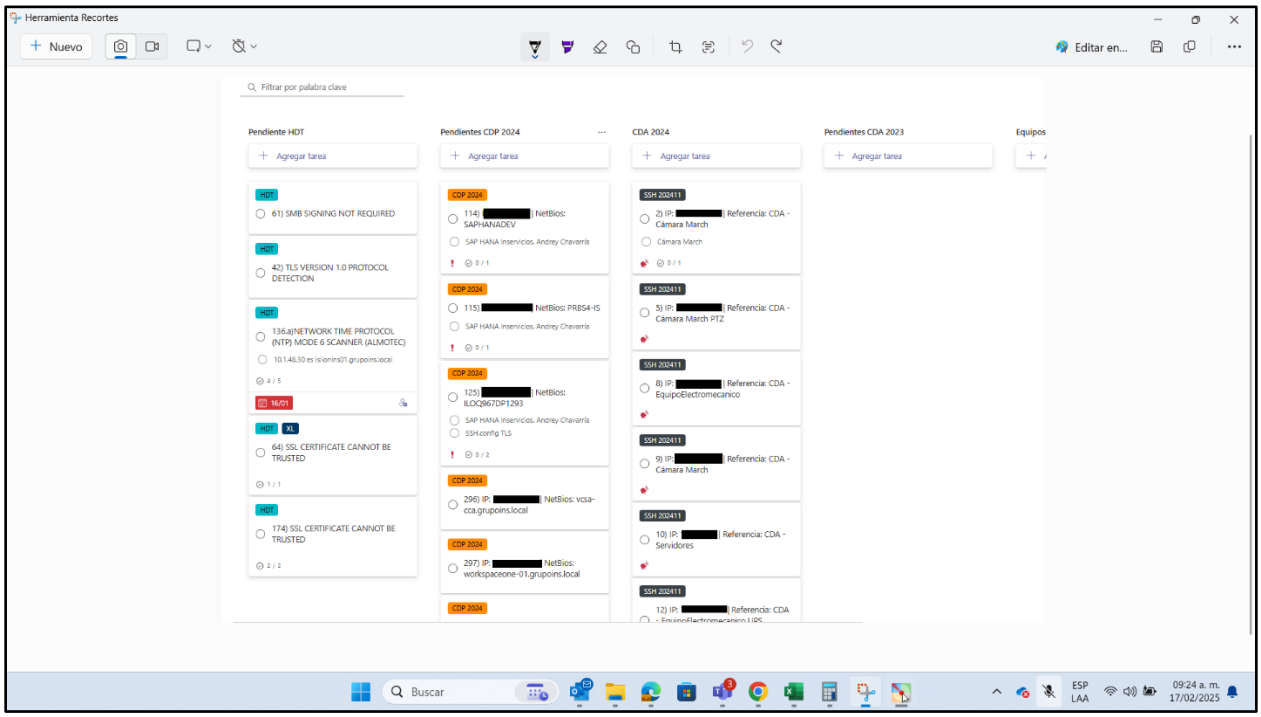
- Infraestructura: existen políticas de acceso a los servidores solamente por parte de los administradores, aparte de los trabajos regulares de mantenimiento que se realizan como parte de la seguridad propia de los equipos.

Reportes obtenidos del tablero Kanvan

Se obtienen diferentes reportes de las atenciones y movimientos realizados por el Grupo Chirripó, en cuanto a la atención de tarjetas de vulnerabilidades, en la siguiente imagen se muestra el estado actual del tablero:

Figura 45

Tablero Kanban Grupo Chirripó.



Las tarjetas están divididas de acuerdo con su estado y ubicación, por ejemplo:

- Pendiente HDT: tarjetas pendientes de atención en la infraestructura del Hospital de Trauma (HDT)
- Pendientes CDP 2024: tarjetas pendientes del Centro de Datos Principal (CDP)
- CDA: Tarjetas atendidas del Centro de Datos Alterno (CDA)
- Pendientes CDA 2023: tarjetas pendientes de atención del Centro de Datos Alterno del año 2023.

Reportes obtenidos de la herramienta Nessus

Debido a la confidencialidad de la información que se emite en los reportes generados de los escaneos de la herramienta Nessus, no es posible mostrar en este documento información

actual, sin embargo, con el fin de documentar y ejemplificar los reportes que se generan con esta, se muestra la siguiente imagen que corresponde a uno de estos reportes:

Figura 46

Reporte Nessus

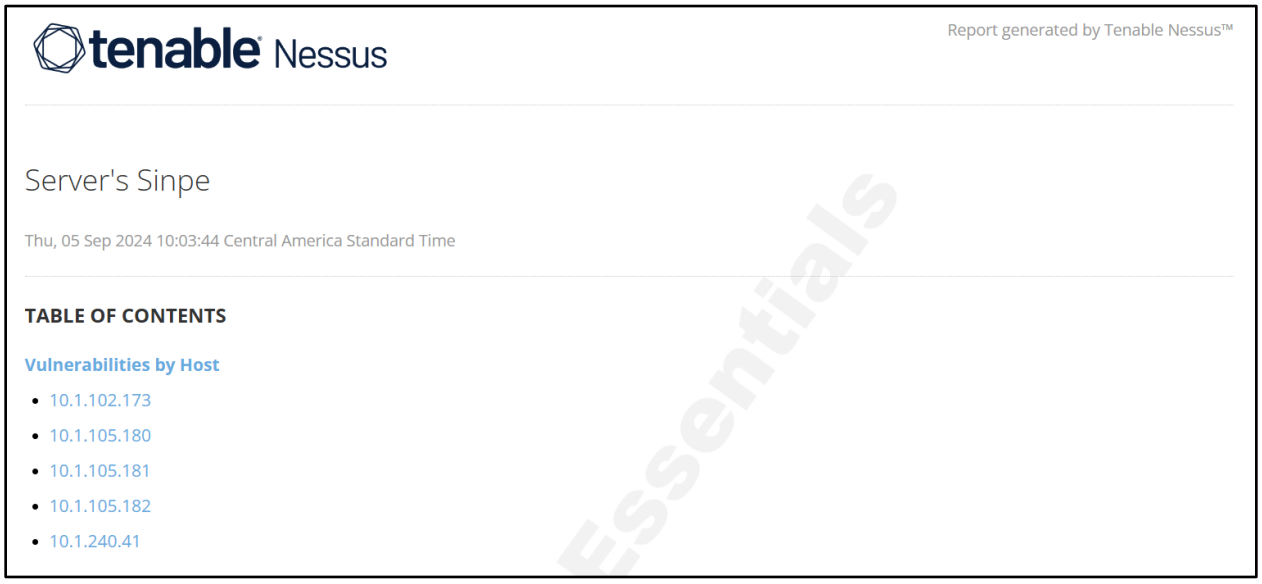
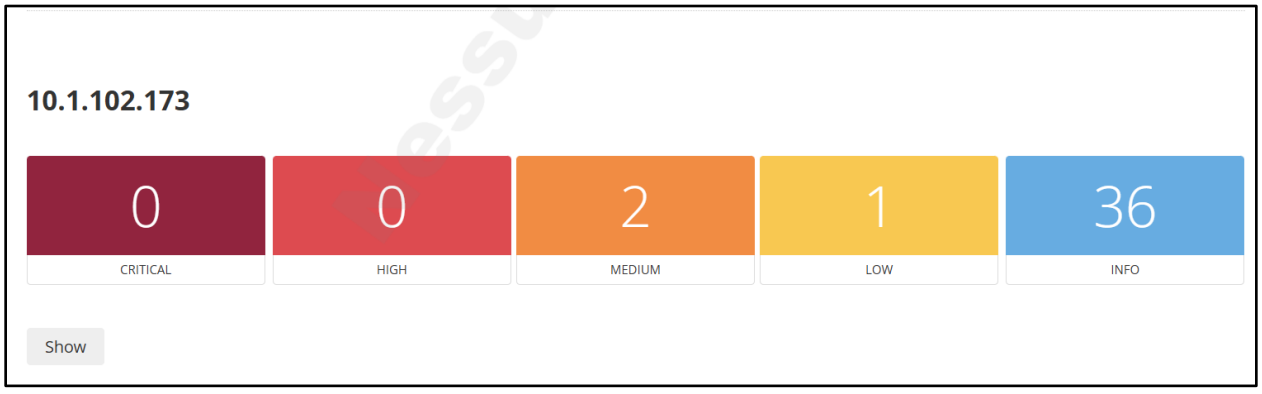


Figura 47

Reporte Nessus Parte 2



Análisis de herramientas tecnológicas utilizadas

Nessus

La herramienta Nessus es un escáner de vulnerabilidades de red, una herramienta que busca debilidades en los sistemas informáticos y redes. Se utiliza para identificar y analizar vulnerabilidades de seguridad en sistemas operativos, aplicaciones y dispositivos de red, es capaz de escanear todo tipo de dispositivos, desde servidores hasta dispositivos móviles, routers y firewalls. (Tenable, 2023)

En el INS, esta herramienta es ejecutada para realizar los escaneos sobre la infraestructura tecnológica, los cuales alimentan los tableros Kanvan utilizados por el equipo Chirripó para la atención de vulnerabilidades. Los escaneos son realizados con una periodicidad mensual, con el fin de mantener actualizada la información, sin embargo, se pueden realizar en cualquier momento para verificar soluciones aplicadas en los equipos.

Kanban (tablero)

Un tablero Kanban es una herramienta ágil de gestión de proyectos diseñada para ayudar a visualizar el trabajo, limitar el trabajo en curso y maximizar la eficiencia (o el flujo). Puede ayudar tanto a los equipos ágiles como a los DevOps a definir el orden de su trabajo diario. Los tableros de Kanban utilizan tarjetas, columnas y la mejora continua para ayudar a los equipos tecnológicos y de servicios a comprometerse con la cantidad de trabajo adecuada y por supuesto, a llevarla a cabo. (Atlassian, 2024)

El equipo Chirripó de atención de vulnerabilidades utiliza el tablero Kanban, que brinda la herramienta Microsoft Planner, esto brinda orden y control en la atención de tarjetas. Las tarjetas son organizadas de acuerdo con su nivel de criticidad, en altas, medias y bajas, esto le permite al equipo brindar la atención oportuna de estas.

Microsoft Azure

Es una plataforma de servicios en la nube que permite a las empresas crear, ejecutar y administrar aplicaciones. Ofrece una variedad de servicios, como almacenamiento, bases de datos, análisis, redes y máquinas virtuales. Azure es una nube pública, lo que significa que los usuarios comparten el hardware, el almacenamiento y las redes con otras organizaciones. (Azure, 2024)

La importancia de esta herramienta en el proceso de detección y corrección de vulnerabilidades radica en que el 95 % de la infraestructura de servidores del INS, es virtual y se encuentra alojada en la solución llamada Azure Vmware Solution (AVS), esto hace que una de las posibles soluciones a implementar en la automatización de procesos ligados a las vulnerabilidades, sea la implementación del Azure Update Manager.

Aranda (Gestión de incidentes)

Es una herramienta que permite gestionar procesos y solicitudes de servicio en una empresa. Esta herramienta ayuda a brindar soporte a clientes y a administrar los recursos tecnológicos de la organización. Es una herramienta que puede ayudar a empresas a mejorar la satisfacción del cliente, reducir costos, identificar oportunidades de mejora, integrar y administrar cambios.

La importancia de esta herramienta en el proceso es que Aranda es utilizado para la gestión de incidentes, esto es algo ligado en muchos casos a vulnerabilidades, además, brinda estadísticas y dashboards que son importantes para obtener datos relativos a estos incidentes.

Estudios de otras organizaciones

A nivel internacional existen varios casos de éxito en empresas del sector de seguros que han automatizado procesos de detección y corrección de vulnerabilidades, a continuación, se van a analizar 3 de estos casos:

1. AXA

AXA es una compañía aseguradora con sede en España, cuenta con más de 147 mil empleados, más de 93 millones de clientes y tiene operaciones en más de 51 países, con una notable presencia en Europa, América, África y Asia, gestiona para sus clientes sus seguros, protección financiera, ahorros e inversiones inmobiliarias dando servicio a sus necesidades. (AXA, 2021)

AXA ha utilizado herramientas de automatización para la gestión de riesgos cibernéticos y la detección de vulnerabilidades. Se utilizaron plataformas de análisis de seguridad como Tenable.io, para identificar vulnerabilidades en sus sistemas y mejorar la protección de datos de sus clientes que son la razón principal de sus operaciones. Al automatizar el proceso de escaneo y evaluación de vulnerabilidades, AXA pudo identificar riesgos potenciales de manera proactiva, lo que redujo significativamente el tiempo necesario para mitigar las amenazas. (AXA, 2021)

2. Metlife

Metlife es un líder global en el campo de los seguros, que además brinda múltiples beneficios a sus empleados. A través de sus subsidiarias y afiliados, mantiene posiciones de liderazgo en el mercado de los Estados Unidos, Japón, América Latina, Asia, Europa, el medio oeste y África. Esta empresa cuenta con 153 años de experiencia, es un líder en innovación y en planes de protección, así como en fondos de pensiones alrededor del mundo. A nivel global se ofrecen seguros de vida, accidentes y salud, también planes de ahorro y de fondos de pensiones,

es una empresa que trabaja con familias, corporaciones y también gobiernos, para brindarles soluciones que les ofrezcan garantías financieras en sus vidas. (MetLife, 2024)

MetLife implementó sistemas de inteligencia artificial (IA) para la automatización de la detección de vulnerabilidades. Se utilizaron herramientas como Tanium y Qualys, para realizar escaneos en tiempo real y obtener análisis más detallados de sus infraestructuras tecnológicas. Esto permitió identificar posibles brechas de seguridad antes de que pudieran ser explotadas, y automatizar de esta forma el proceso de mitigación de vulnerabilidades.

3. Chubb

Chubb es una empresa líder mundial en seguros, cuenta con operaciones en 54 países y territorios, provee seguros para propiedades personales y comerciales, así como seguro para accidentes, y seguros de salud complementarios, reaseguramiento y seguros de vida para un grupo diverso de clientes. La compañía es definida por su extensa oferta de productos y servicios, excelentes capacidades de mercadeo, excepcional fortaleza financiera y operaciones locales a nivel global. Es una empresa que forma parte del S&P 500 index, cuenta con aproximadamente 40000 empleados a nivel global. (Chubb, 2024)

Adicionalmente es importante destacar que Chubb es un socio comercial muy destacado e importante para el Instituto Nacional de Seguros (INS) desde hace varios años.

Chubb implementó un sistema automatizado de pruebas de penetración para mejorar la seguridad de sus aplicaciones y redes. Utilizando herramientas como Burp Suite y Nessus, automatizó la detección de vulnerabilidades en sus sistemas, lo que les permitió reducir significativamente los tiempos de respuesta y mejorar la protección contra ataques. Además, esto les permitió gestionar de manera más eficiente el cumplimiento de las normativas de seguridad existentes.

Análisis de benchmarking de normas internacionales aplicables

En la siguiente matriz se muestra una descripción de las normas internacionales aplicables a la detección y corrección de vulnerabilidades, con el fin de determinar la o las más adecuadas para aplicar en este proyecto:

Tabla 3

Análisis de normas internacionales

Norma Internacional	Organismo	Área de Aplicación	Descripción
ISO/IEC 27001:2013	ISO (International Organization for Standarization)	Seguridad de TI	Establece requisitos para un sistema de gestión de la información, incluyendo la gestión de vulnerabilidades en TI.
ISO/IEC 27002:2022	ISO	Seguridad de TI	Brinda pautas para la implementación de controles de seguridad, incluyendo la gestión de vulnerabilidades y parches.

ISO/IEC 29147:2018	ISO	Gestión de vulnerabilidades	Brinda directrices para la divulgación responsable de vulnerabilidades, abarcando el proceso de identificación, evaluación y comunicación.
NIST SP 800-53	NIST (National Institute of Standards and Technology)	Gestión de la Seguridad en sistemas informáticos	Especifica controles de seguridad que incluyen la identificación, evaluación y mitigación de vulnerabilidades en sistemas informáticos y redes.
NIST SP 800-115	NIST	Pruebas de seguridad (Pruebas de penetración)	Brinda directrices para la realización de pruebas de penetración y la evaluación de la seguridad de los

			sistemas para identificar vulnerabilidades.
OWASP Top Ten	OWASP (Open Web Application Security Project)	Seguridad en aplicaciones web	Brinda un listado de las 10 principales vulnerabilidades de seguridad en aplicaciones web y las mejores prácticas para mitigarlas
CIS Controls (Center for Internet Security)	CIS	Seguridad de TI	Define un conjunto de controles de seguridad cibernética prioritarios que incluyen la gestión de vulnerabilidades y la protección de activos informáticos.
PCI DSS (Payment Card Industry Data Security Standard)	PCI Security Standards Council	Seguridad en pagos electrónicos	Establece requisitos para proteger los datos de tarjetas de pago, incluyendo la gestión de las

			vulnerabilidades y la aplicación de parches en sistemas de pago.
ISO/IEC 27005:2018	ISO	Gestión de riesgos en la seguridad de la información	Establece directrices para la gestión de riesgos, incluyendo la identificación de vulnerabilidades y la evaluación de sus impactos en la seguridad de la información.

Nota. Fuente: (INCIBE, 2024)

A parir de la comparación de las características clave, las normas y marcos que mejor se adaptan a el requerimiento de automatización de atención de vulnerabilidades del INS son ISO/IEC 27001 y NIST SP 800-53. Ambas ofrecen una cobertura amplia, permiten integración con otros marcos, y son altamente relevantes para organizaciones que buscan gestionar la seguridad de la información de manera integral.

- ISO/IEC 27001 es la mejor alternativa para organizaciones que buscan una certificación formal y que tienen los recursos necesarios para implementar un SGSI completo y gestionar sus riesgos de manera continua.

- NIST SP 800-53 es la mejor opción para organizaciones que desean un enfoque flexible y centrado en la resiliencia cibernética, sin necesidad de certificación oficial, pero con un enfoque claro en la gestión de riesgos y la protección de infraestructuras críticas, además se enfoca en controles de seguridad que incluyen la identificación, evaluación y mitigación de vulnerabilidades en sistemas informáticos y redes.

Estudio de factibilidad

Resumen Ejecutivo

Antecedentes del proyecto

Este proyecto se basa en la necesidad existente de mejorar por medio de la automatización de procesos, las labores que se realizan en el Instituto Nacional de Seguros (INS) para la detección y corrección de vulnerabilidades en la infraestructura tecnológica.

Si bien es cierto existe ya un proceso establecido para la detección y corrección de estas vulnerabilidades, la gran mayoría de las labores que lo componen son procesos manuales, esto conlleva una serie de riesgos que deben ser tomados en cuenta y en los cuales, la automatización puede brindar un espacio de mejora muy importante.

Tomando en cuenta aspectos legales, contractuales y económicos, parte de la idea de este proyecto, es la de utilizar recursos y herramientas con las que el INS ya cuenta y que permitan la automatización de algunos procesos que están involucrados directamente con la corrección y protección de la infraestructura tecnológica, esto con el fin de aprovechar dichos recursos y minimizar los costos asociados a esta propuesta.

Este proyecto es del interés de la organización, especialmente de la Dirección de Tecnologías de Información, como encargada de la infraestructura tecnológica, por lo que es una propuesta que será de sumo interés para las jefaturas correspondientes.

Hasta el momento se han realizado entrevistas, encuestas e investigaciones, respecto de las herramientas disponibles que pueden ser utilizadas, así como análisis de otras herramientas existentes en el mercado, que pueden ser presentadas como posibles opciones de solución en este proyecto.

Descripción del proyecto

El propósito principal de este proyecto es del aportar una propuesta para la automatización de algunos procesos ligados a la detección y corrección de vulnerabilidades en la infraestructura tecnológica en el Instituto Nacional de Seguros (INS). Esta propuesta incluirá tanto aspectos de utilización de herramientas internas existentes y de las cuales se cuenta con licencia, como la propuesta de uso de herramientas existentes en el mercado y que se pueden ajustar a la propuesta de esta investigación.

Objetivos

- Automatizar procesos
- Presentar propuesta
- Realizar laboratorios

Contexto del proyecto

El Instituto Nacional de Seguros (INS) es una entidad oficial que se dedica a la comercialización de seguros como principal fuente de ingreso. Tiene 100 años de existencia y una sólida base económica y de infraestructura que la hace ser una de las aseguradoras más importantes de Latinoamérica. Desde este punto de vista la seguridad es un aspecto básico, pues

es la base fundamental sobre la cual se apoyan los clientes, de ahí que contar con una infraestructura tecnológica robusta y protegida es vital para la organización.

Además, la protección de la infraestructura tecnológica por medio de la detección y corrección de vulnerabilidades es una actividad impulsada por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, que es el máximo ente en materia de Tecnología a nivel gubernamental.

La participación en el proceso de detección y corrección de vulnerabilidades, mediante la integración del grupo denominado Chirripó, que es una célula interna conformada por funcionarios técnicos expertos de varias áreas de la Dirección de Tecnologías de Información, brindó la visión de innovar y ayudar en el proceso mediante la automatización de algunas de las tareas, esto dio origen a este proyecto.

Alcance del estudio de factibilidad

Se espera de este estudio obtener la aprobación de las jefaturas para que se puedan aplicar algunas de las propuestas que se brindarán en el proyecto, y demostrar la factibilidad de realizar y aplicar dichos cambios, demostrando su factibilidad en todos los aspectos necesarios.

Con el fin de preparar la evaluación de la factibilidad de este proyecto, se realizaron varias investigaciones a nivel de productos existentes en el mercado, que pueden ser objetos de ser valorados para su uso en el INS, además se realizó una encuesta y dos entrevistas con personal clave en el proceso, para obtener un panorama más claro de la situación actual y de la visión existente con respecto a la automatización de procesos.

La aprobación de esta propuesta es decisión de la Dirección de Tecnologías de Información del INS, y de la Jefatura del Departamento de Operaciones y Soporte Técnico que

se encargan del proceso de detección y corrección de vulnerabilidades, así como de administrar la infraestructura tecnológica.

Factibilidad técnica

Para la realización de este proyecto es importante tener en cuenta la infraestructura tecnológica existente en el INS actualmente, esto permitirá tener claro el alcance de este, por lo tanto, se detallan a continuación los principales aspectos:

- Servidores: se cuenta con servidores virtuales en un 98 % de la infraestructura, de los sistemas operativos Microsft Windows, Red Hat Linux y Unix.
- La plataforma es hibrida, pues se cuenta con servidores On Premise que están alojados en servidores físicos ubicados en los Centros de Datos del INS, así como también servidores ubicados en la nube de Azure mediante la solución (Azure Vmware Solution), en ambos casos la plataforma utilizada para alojar las máquinas virtuales es VmWare.
- Actualmente, se utiliza para el escaneo de vulnerabilidades la herramienta Nessus, la cual ha brindado buenos resultados.
- Se ha hecho la investigación de otras herramientas existentes que realizan el escaneo de vulnerabilidades en estas plataformas, las principales son: intruder, ManageEngine, Teramind, Paessler, OpenVAS, etc.
- De acuerdo con lo investigado estas herramientas pueden integrarse con los sistemas actuales.
- Al contar con un amplio porcentaje de la infraestructura en plataforma virtual, existe la posibilidad de utilizar herramientas propias de Azure, que permitan

automatizar algunos de los procesos, por ejemplo, el Azure Update Manager, que permite automatizar la aplicación de los updates de Windows en estos servidores, también el VMWare permite crear guías de hardenización para la creación de plantillas para servidores con las especificaciones de seguridad requeridas.

Factibilidad económica

Con esta propuesta de automatización de procesos, se busca no solo innovar en el proceso de detección y corrección de vulnerabilidades, sino también, mejorar aspectos como limitar el error humano.

Sin embargo, se cree que uno de los factores principales es el ahorro que se puede realizar desde la parte económica, para esto se propone la utilización de herramientas con las que la institución ya cuenta, y que no son aprovechadas en su totalidad, esto no generaría un costo adicional en licenciamiento, por ejemplo, pero si implica un ahorro en recursos de horas extras para la aplicación de parches de Windows.

Se observa este dato con un ejemplo:

Proceso actual:

- 5 recursos durante 12 horas de parchado = 1.300.000 colones de importe en horas extras mensual.

Con automatización de proceso de parchado:

- 1 recurso durante 3 horas para revisión = 46.620 colones de importe en horas extras mensual.

Esto representa un ahorro de recursos económicos importante en el rubro de horas extras, esto repercute positivamente no solo en los recursos de la institución, sino en la carga laboral de los funcionarios.

Cálculo del VAN y TIR:

Año	Flujo de caja			
0	-22000			
1	8000		**24%**	**TIR**
2	8000		**$7 569,36**	**VAN**
3	8000			
4	8000			
5	8000			

El flujo inicial de $22000 representa el monto pagado en horas extras a 5 funcionarios en un año, luego la inversión a realizar bajará debido a la automatización de procesos a $8000 por año, de ahí los valores de TIR y VAN obtenidos para el proyecto.

Factibilidad Legal

Dado que la propuesta se basa en la utilización de herramientas existentes y para las cuales el INS ya cuenta con licenciamiento (Azure, Nessus), no se prevén problemas en el aspecto legal para este proyecto.

De igual forma, en caso de que en algún momento se decida a utilizar alguna de las herramientas que se proponen, se debe solamente cumplir con el procedimiento establecido para estos propósitos en las instituciones del estado, estableciendo el concurso respectivo y en el cual deben existir al menos 3 proveedores para adjudicar el contrato respectivo.

Factibilidad de recursos

Se cuenta con los recursos necesarios para la realización del proyecto, actualmente participan 6 recursos en el grupo llamado Chirripó para la atención de vulnerabilidades, además

de dos recursos del área de Seguridad de TI que se encargan de la realización de los escaneos, de tal forma que la factibilidad de recursos humanos necesarios para el proyecto está garantizada.

Desde el punto de vista de infraestructura, al tratarse un proyecto que se ejecuta sobre la plataforma actual existente, no existen tampoco factores que puedan afectar.

El único proceso que se vería alterado con la aplicación de este proyecto en principio sería la parte de la aplicación de parches de Windows, pues se reduciría considerablemente la cantidad de recursos necesarios para realizarlo.

Factibilidad de mercado

El mercado existente en el campo de la automatización de procesos para la detección y corrección de vulnerabilidades, principalmente en el primer aspecto, tomando en cuenta que algunos de las tareas de corrección aún siguen siendo muy manuales, es amplio, teniendo en cuenta que la seguridad de la infraestructura tecnológica de las empresas es ahora uno de los puntos principales que se tienen en cuenta.

En la siguiente imagen se ilustran algunos de ellos, sin embargo, en este sentido la oferta es muy amplia:

Figura 48

Software para detección de vulnerabilidades

Nota.Fuente (guru99, 2023)

Factibilidad operacional

Debido a que el proceso de detección y corrección de vulnerabilidades debe realizarse siempre, su factibilidad operacional está supeditada a la aplicación de correcciones en servidores que soportan sistemas que son considerados como críticos en la Institución.

La disponibilidad de estos sistemas críticos es una prioridad para la administración superior, de ahí que cualquier interrupción debe ser ampliamente calculada y planificada, esto para no afectar la operativa y principalmente para no afectar a los usuarios.

La aplicación de parches de Windows se realiza una vez al mes, el tercer sábado de cada mes, la corrección de vulnerabilidades se realiza dos veces a la semana en sesiones específicas

para este fin, siempre y cuando no representen alguna interrupción, en ese caso debe planificarse de acuerdo con lo indicado anteriormente.

De esta forma, cualquier herramienta adicional que puede o deba ser agregada a la plataforma con estos fines, debe ajustarse a estos lineamientos.

Factibilidad de tiempo

Se planifica el contar con resultados derivados de este proyecto en los próximos tres meses, la propuesta inicial indicará el iniciar con la configuración y aplicación de la automatización del proceso de parchado de servidores Windows, de tal forma que en este tiempo dicha herramienta pueda ser configurada y probada en la plataforma, sobre los equipos del ambiente de desarrollo, para posteriormente aplicarlo en la parte productiva.

Para llegar a este punto se debe instalar en los servidores un agente del Azure Arc, que permita hacer la conexión con el Azure Update Manager para la configuración y aplicación de los parches, por lo tanto, este proceso es el que puede requerir más tiempo para lograr tener todos los equipos registrados en Azure Arc.

Paralelamente se estará trabajado en las guías de hardenización para la creación de servidores nuevos, buscando con esto que se puede automatizar este proceso de puesta a punto de los equipos y cuando sean dados de alta ya cuenten con todas las especificaciones de seguridad requeridas al momento.

Análisis de riesgos

Se presenta seguidamente el análisis de riesgos identificados para el proyecto:

Tabla 4

Análisis de riesgo

Riesgo	Probabilidad	Impacto	Nivel de Riesgo	Planta de Mitigación	Valor de Riesgo Residual
Fuga de datos confidenciales	Alta	Alto	Critico	Implementación de cifrado en reposo y tránsito, autenticación multifactor, formación al personal.	Bajo
Ataque de Ransonware	Media	Alto	Alto	Copias de seguridad frecuentes, uso de software antivirus actualizado, segmentación de la red.	Medio

Acceso no autorizado a sistemas críticos	Baja	Muy alto	Alto	Implementación de controles de acceso estrictos, revisión de permisos de usuarios, auditoría de accesos	Bajo
Interrupción del servicio por fallos de infraestructura	Alta	Medio	Alto	Redundancia de infraestructura, mantenimiento preventivo regular, pruebas de recuperación ante desastres.	Bajo
Vulnerabilidades en aplicaciones web	Alta	Medio	Alto	Pruebas de penetración periódicas, implementación de prácticas de desarrollo seguro, parches rápidos.	Medio

Falta de cumplimiento con regulaciones de protección de datos	Media	Alto	Alto	Actualización constante de políticas de privacidad, auditorías periódicas de cumplimiento, capacitación regular al personal.	Medio
Errores humanos en la gestión de TI	Alta	Bajo	Medio	Automatización de procesos críticos, capacitación continua, supervisión de actividades de TI.	Bajo
Mala práctica de compartir contraseñas para acceso a sistemas	Media	Alto	Alto	Políticas estrictas de acceso, solicitud de cambio de clave	Medio

				mensual, ver la posibilidad de agregar un factor adicional de autenticación.	

Mapa de calor:

MUY ALTA	MUY ALTAMUY BAJA	MUY ALTABAJA	MUY ALTAMEDIA	MUY ALTAALTA	MUY ALTAMUY ALTA
ALTA	ALTAMUY BAJA	ALTABAJA	ALTAMEDIA	ALTAALTA	ALTAMUY ALTA
MEDIA	MEDIAMUY BAJA	MEDIABAJA	MEDIAMEDIA	MEDIAALTA	MEDIAMUY ALTA
BAJA	BAJAMUY BAJA	BAJABAJA	BAJAMEDIA	BAJAALTA	BAJAMUY ALTA
MUY BAJA	MUY BAJAMUY BAJA	MUY BAJABAJA	MUY BAJAMEDIA	MUY BAJAALTA	MUY BAJAMUY ALTA
	MUY BAJA	**BAJA**	**MEDIA**	**ALTA**	**MUY ALTA**

	Probabilidad	Impacto	LLAVE	Zona de riesgo
1	ALTA	ALTA	ALTAALTA	MUY ALTA
2	MEDIA	ALTA	MEDIAALTA	MUY ALTA
3	BAJA	MUY ALTA	BAJAMUY ALTA	MUY ALTA
4	ALTA	MEDIA	ALTAMEDIA	ALTO
5	ALTA	MEDIA	ALTAMEDIA	ALTO
6	MEDIA	ALTA	MEDIAALTA	MUY ALTA
7	ALTA	BAJA	ALTABAJA	ALTO
8	MEDIA	ALTA	MEDIAALTA	MUY ALTA

ROJO	MUY ALTO
NARANJA	ALTO
AMARILLO	MEDIO
VERDE	BAJO

De acuerdo con lo observado en el mapa de calor, se llega al siguiente análisis: el hecho de que existan zonas con riesgos altos y muy altos implica que existen áreas que requieren una atención inmediata con el fin de mitigar las amenazas en aspectos de seguridad, estabilidad y operativa de la infraestructura de la institución.

En cuanto a los riesgos muy altos representan zonas que pueden causar un impacto importante en la operativa de la institución y la disponibilidad de los servicios que brinda.

Respecto a los riesgos altos, representan amenazas que no son tan severas, pero que, si pueden representar interrupciones o pérdidas menores en los servicios, por lo tanto, deben ser tomadas en cuenta de la misma forma y con bastante importancia.

Análisis de benchmarking de tecnologías en ciberseguridad

A continuación, se presenta el análisis de benchmarking realizado con las diferentes herramientas tecnológicas existentes en el mercado en materia de ciberseguridad:

Tabla 5

Análisis de benchmarking de herramientas tecnológicas de ciberseguridad.

Herramienta	Tipo de vulnerabilidades	Método de escaneo	Automatización	Integración	Facilidad de uso	Cobertura de normas	Costo	Rendimiento
Tenable Nessus	Red, aplicaciones, sistemas operativos	Activo	Alta, con reportes detallados y configuraciones personalizables	Compatible con plataformas SIEM y otras herramientas de gestión.	Interfaz amigable, fácil de configurar	Compatible con regulaciones como PCI DSS, HIPAA,etc.	Licencia de pago, con versión de prueba	Rápido y eficiente, pero puede consumir recursos durante escaneos grandes.

OpenVAS	Red, aplicaciones, servicios.	Activo	Escaneos programables, reportes detallados	Compatible con otras herramientas, aunque tiene más limitaciones que Nessus.	Interfaz, no tan amigable, pero es funcional.	Cumple con estándares comunes.	Gratuita, código abierto.	Requiere recursos considerables pero adecuado para entornos pequeños a medianos.
Qualys	Red, aplicaciones, dispositivos.	Activo y Pasivo.	Muy alta con una amplia gama de opciones para informes automáticos	Buena integración con plataformas de gestión de seguridad.	Interfaz web intuititva.	Cumple con marcos regulatorios internacionales.	Basado en suscripción, con planes escalables.	Excelente rendimiento, en la nube, no requiere infraestructura propia.

Burp Suite	Aplicaciones Web	Activo (pruebas de penetración)	Funcionalidades de automatización limitadas en comparación con otras	Compatible con herramientas de seguridad adicionales, como CI/CD.	Requiere conocimientos técnicos avanzados.	Soporta pruebas enmarcadas en OWASP.	Gratuita (versión básica) y de pago (versión profesional).	Funciona bien en entornos con aplicaciones web dinámicas.
Nikto	Aplicaciones web, servidores web.	Activo	Funcionalidad limitada, pero es útil para escaneos rápidos.	No tan integrada como otras herramientas, pero compatible con herramient	Basada en línea de comandos, menos accesible para novatos.	Puede detectar una variedad de configuraciones erróneas, pero no sigue estrictamente	Gratuita y de código abierto	Ligera, pero no tan completa como otras herramientas de escaneo

				as de análisis		marcos como OWASP		

Como conclusiones, y viéndolo desde la óptica institucional, se presenta lo siguiente:

- Nessus y Qualys representan las opciones más robustas para una detección completa de vulnerabilidades con un enfoque más empresarial, aunque son las herramientas más costosas.
- OpenVAS es una excelente opción si se busca una herramienta gratuita con buen desempeño, aunque puede ser un poco más compleja de usar, sin embargo, en el INS no es muy probable utilizar herramientas gratuitas.
- Burp Suite es una herramienta ideal para la seguridad de aplicaciones web, sobre todo si se realizan pruebas de penetración manuales, sin embargo, este proyecto está más orientado a infraestructura y no a aplicaciones.
- Nikto es adecuada para escaneos rápidos y sencillos en servidores web, pero sin la profundidad de otras herramientas.

CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

La automatización del proceso de detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS) representa un avance significativo en la optimización de la seguridad informática y la minimización de riesgos asociados a ciberataques.

5.1. Conclusiones

A partir del análisis realizado en este estudio, se han identificado una serie de conclusiones clave. Con base en los resultados obtenidos se emiten las siguientes conclusiones obtenidas del trabajo de investigación:

- Se logró identificar por medio de las encuestas y las entrevistas que es viable proponer un modelo en el cual se incluya la automatización como un componente adicional dentro del proceso de detección y corrección de vulnerabilidades establecido en el INS.
- Se logra analizar diferentes herramientas tecnológicas existentes en el mercado que brindan un panorama más amplio de las posibilidades con que se cuenta y que pueden ayudar a establecer una comparación para una utilización futura.
- Se determinó que los procesos actuales del departamento de Operaciones y Soporte Técnico presentan oportunidades de mejora, principalmente en la eficiencia de la identificación y mitigación de vulnerabilidades. Se evidenció que el tiempo de respuesta ante amenazas puede reducirse significativamente mediante la automatización de tareas repetitivas y el uso de herramientas avanzadas de escaneo y corrección.

- La implementación de un modelo automatizado debe alinearse con estándares internacionales de seguridad como ISO 27001, NIST 800-53 y el marco MITRE ATT&CK. Se identificó que la adopción de estos estándares permite mejorar la eficacia del proceso y garantizar el cumplimiento normativo.
- La automatización de la detección y corrección de vulnerabilidades puede beneficiarse del uso de plataformas como Tenable Nessus, Qualys, OpenVAS y herramientas de gestión de parches como Ansible y SCCM. La integración de estas soluciones en un flujo de trabajo unificado optimiza la identificación de riesgos y agiliza su mitigación.

  Se evidenció que la implementación de metodologías ágiles, como DevSecOps, permite mejorar la respuesta a vulnerabilidades al integrar la seguridad dentro del ciclo de vida del desarrollo y operación de sistemas. Esto favorece la detección temprana y la aplicación de parches de manera oportuna.
- La automatización reduce la carga operativa del personal de seguridad, permitiendo que se concentren en actividades estratégicas. Además, minimiza errores humanos al eliminar la dependencia exclusiva de revisiones manuales, lo que resulta en una gestión más efectiva de las amenazas.
- Se logra determinar que existe amplia aceptación en cuanto al proceso de detección y corrección de vulnerabilidades actual, sin embargo, siempre con aspectos de mejora que se deben aplicar.

- Se logra observar que existe amplitud en la organización para implementar la automatización en procesos ligados a la detección y corrección de vulnerabilidades,

sin embargo, existen algunas limitantes en aspectos de adquisición de software entre otros que impiden que esto sea realizado de manera inmediata.

- Existe amplia confianza en las herramientas actuales utilizadas para este proceso, tanto para el escaneo de la infraestructura como para el control de las tarjetas atendidas.
- Los procesos actuales de corrección de vulnerabilidades, así como procesos alternos que intervienen en esta labor, por ejemplo, el parchado de servidores son manuales, de tal forma que la posibilidad de implementar la automatización es importante para mejorar en los tiempos de atención.
- Se logra determinar que existe una infraestructura adecuada para soportar un modelo automatizado para la detección y corrección de vulnerabilidades.
- Se logra determinar que existe apertura desde la parte administrativa y gerencial para incorporar la automatización en procesos dentro de la institución, realizándolo de manera gradual y sin comprometer la operativa diaria.
- Se logran identificar los estándares internacionales aplicables a la gestión de seguridad informática en el INS, siempre ajustados a las normativas emitidas por el gobierno al ser una institución de corte gubernamental.
- Se logran identificar procesos que pueden ser automatizados utilizando herramientas que ya existen y están a disposición de la institución, con el fin de elaborar la propuesta.

- Se logra determinar basado en las encuestas y entrevistas realizadas, que la automatización de procesos en materia de detección y corrección de vulnerabilidades tiene aceptación dentro de la parte técnica de la institución.
- Se logra determinar que existen varias herramientas que permiten la gestión de las vulnerabilidades en la infraestructura tecnológica mediante metodologías ágiles, que pueden ser incorporadas al proceso y a la propuesta.

5.2.Recomendaciones

Tomando como base la investigación realizada y luego de llegar a las conclusiones anteriormente mencionadas, se generan las siguientes recomendaciones:

- Se recomienda implementar la automatización de manera gradual, comenzando con un programa piloto que permita evaluar la efectividad de las herramientas seleccionadas antes de una implementación completa a nivel institucional.
- Es fundamental capacitar al personal del departamento de Operaciones y Soporte Técnico en el uso de herramientas de automatización y mejores prácticas de ciberseguridad, garantizando una transición eficiente y una correcta interpretación de los reportes generados por los sistemas automáticos.
- Se recomienda la creación o fortalecimiento de un Centro de Operaciones de Seguridad (SOC) que supervise en tiempo real la gestión de vulnerabilidades, permitiendo una respuesta más rápida y efectiva ante amenazas (Ya existe bajo contrato con GBM).

- La incorporación de algoritmos de inteligencia artificial puede mejorar la detección de patrones anómalos y predecir vulnerabilidades futuras, lo que permitiría un enfoque proactivo en la seguridad del INS.
- Es recomendable establecer auditorías y evaluaciones periódicas del modelo automatizado para asegurar su eficacia y adaptabilidad ante nuevas amenazas y cambios en la infraestructura tecnológica del INS.
- Se sugiere la integración del sistema automatizado con herramientas SIEM para una mejor correlación y análisis de eventos de seguridad, permitiendo una toma de decisiones basada en datos en tiempo real.
- Se debe garantizar que la automatización cumpla con los requerimientos regulatorios nacionales e internacionales, estableciendo políticas de seguridad robustas y alineadas con los estándares de la industria.
- La implementación de un monitoreo continuo con herramientas de automatización debe complementarse con un plan de respuesta a incidentes eficiente, asegurando que cualquier vulnerabilidad detectada sea abordada de manera inmediata y efectiva.

CAPÍTULO 6: PROPUESTA DE DISEÑO

6.1 Introducción

Este capítulo presenta la propuesta de diseño del modelo automatizado para la detección y corrección de vulnerabilidades en la infraestructura tecnológica del Instituto Nacional de Seguros (INS). Se describen los elementos clave de la solución, su arquitectura, los componentes tecnológicos, los flujos de procesos y la metodología de implementación, basados en resultados obtenidos de la presente investigación.

6.2 Diagnóstico de la situación actual

Se realizó un análisis detallado de los procesos actuales utilizados por el departamento de Operaciones y Soporte Técnico para la detección y corrección de vulnerabilidades. Este diagnóstico incluyó:

- Evaluación de herramientas utilizadas actualmente para escaneo y gestión de vulnerabilidades.
- Identificación de brechas y limitaciones en la automatización de estos procesos.
- Análisis de tiempos de respuesta y efectividad en la mitigación de vulnerabilidades.
- Revisión de roles y responsabilidades del personal en gestión de seguridad.

Con estos insumos se pudo determinar que existe una herramienta utilizada para el escaneo de la infraestructura tecnológica llamada Nessus que cumple con las expectativas de la institución, se estudiaron otras herramientas existentes en el mercado y que pueden en algún momento ser considerados para su implementación, en este sentido el hecho de que el INS sea una institución

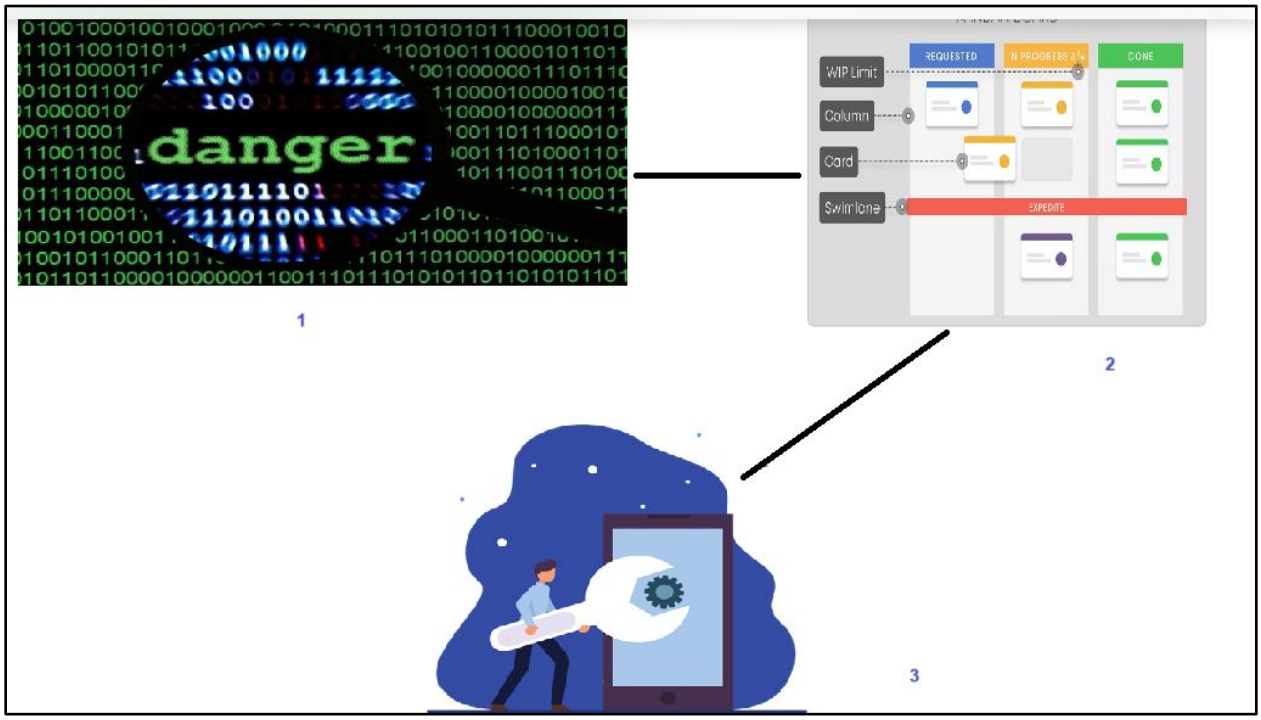
gubernamental hace que deba ajustarse a la normativa vigente y que este proceso de adopción de nuevas tecnologías no sea sencillo de realizar.

Se logra identificar que la automatización puede realizarse de forma parcial en procesos que forman parte de las tareas de corrección de vulnerabilidades y de prevención de estas, por ejemplo, el parchado de servidores Windows, esto puede realizarse con herramientas ya existentes y licenciadas en la institución.

El flujo actual del proceso es el siguiente:

Figura 49

Proceso actual de detección y corrección de vulnerabilidades



1.Escaneo de infraestructura

2.Distribución de casos de vulnerabilidades de acuerdo con su criticidad

3.Corrección de vulnerabilidades.

6.3 Requerimientos y especificaciones técnicas

Con base en el diagnóstico, se establecen los siguientes requerimientos para el modelo automatizado:

6.3.1 Requerimientos funcionales

1. Escaneo de vulnerabilidades:

- Capacidad para realizar escaneos programados y en tiempo real.
- Integración con herramientas de escaneo como Nessus, OpenVAS o Qualys.
- Análisis de configuraciones y detección de configuraciones inseguras.
- Soporte a diferentes tipos de escaneo (red, aplicaciones web, contraseñas)

2.Generación de reportes y análisis:

- Generación automatizada de reportes detallados sobre vulnerabilidades detectadas.
- Priorización de vulnerabilidades según impacto y criticidad.

  Notificación a equipos responsables de seguridad mediante alertas automatizadas.

3.Automatización de corrección:

- Implementación de flujos de trabajo automatizados para la corrección de vulnerabilidades.
- Aplicación de parches de seguridad según criticidad y compatibilidad.
- Integración con herramientas de automatización como Ansible, Puppeto Chef.
- Configuración e implementación del parchado automático de los servidores de la plataforma Windows, por medio de la herramienta Azure Update Manager.

4.Gestión y monitoreo centralizado:

- Registro y auditoría de actividades en un sistema centralizado.
- Panel de control para visualizar estado de seguridad en tiempo real.
- Integración con SIEMs como Splunk o ELK Stack para correlación de eventos.

6.3.2 Requerimientos no funcionales

1. Seguridad:
    - Cifrado de datos en tránsito y en reposo mediante TLS y AES.
    - Control de acceso basado en roles (RBAC) para limitar privilegios de usuario.
    - Cumplimiento con estándares como ISO 27001, NIST y CIS Controls.
    - Utilizar un cifrado de al menos 256 bits.
2. Escalabilidad:
    - Capacidad de adaptación a infraestructuras tecnológicas en expansión.
    - Soporte para múltiples entornos y plataformas heterogéneas.
    - Capacidad de realizar un escaneo completo de vulnerabilidades en una red y en sistemas adicionales, sin degradación en el rendimiento, soportando hasta 10000 dispositivos sin necesidad de rediseñar la infraestructura.
3. Disponibilidad y rendimiento:
    - Alta disponibilidad con balanceo de carga y redundancia.
    - Tiempos de respuesta óptimos para detección y mitigación en tiempo real.
    - Integración con sistemas de monitoreo para detectar fallos en la solución.
    - Realizar un escaneo completo en una red de hasta 500 dispositivos en menos de 2 horas.
    - Estar disponible al menos el 99.9 % del tiempo durante los horarios de operación.
4. Usabilidad y mantenibilidad:
    - Interfaz intuitiva para la administración y supervisión de vulnerabilidades.
    - Documentación clara para la configuración y mantenimiento del sistema.
    - Modularidad para facilitar futuras actualizaciones o mejoras.

- Permitir actualizaciones de la base de datos de vulnerabilidades (CVEs) al menos una vez al mes, sin necesidad de intervención manual en más del 90 % de los casos.
- El sistema debe ser capaz de generar un informe preliminar sobre vulnerabilidades en un máximo de 10 minutos luego de finalizar el escaneo.

Tabla 6

Product Backlog de la propuesta de Automatización.

ID	Historia de Usuario	Prioridad	Criterios de Aceptación	Esfuerzo (en Puntos)
	Evaluar desde el punto de vista de analista de seguridad el estado actual del proceso de detección de vulnerabilidades para identificar áreas de mejora.	Alta	-Generar informa de diagnóstico. -Se identifican herramientas y procesos actuales. -Se documentan brechas de seguridad.	5

HU-02	Desde el punto de vista de arquitecto de software, diseñar la arquitectura del modelo automatizado para garantizar su integración con las herramientas existentes.	Alta	-Se define una arquitectura escalable. -Se validan tecnologías compatibles. -Se documenta la arquitectura del sistema.	8
HU-03	Como ingeniero DevOps, quiero integrar una herramienta de escaneo de	Alta	-La herramienta seleccionada se integra correctamente	13

	vulnerabilidades para que el sistema pueda detectar amenazas automáticamente.		-Se realiza un escaneo de prueba exitoso. -Se generan reportes de vulnerabilidades.	
HU-04	Como desarrollador, quiero automatizar la ejecución de escaneos de vulnerabilidades para reducir la intervención manual	Alta	-Se programan escaneos automáticos periódicos. -Se generan reportes automáticos. -Se integran alertas en caso de	13

			vulnerabilidades críticas.	
HU-05	Como analista de seguridad, quiero recibir alertas en tiempo real cuando se detecten vulnerabilidades críticas para reaccionar rápidamente.	Media.	-Se configuran alertas en el SIEM. -Las alertas contienen detalles de la vulnerabilidad. -Se notifican a los responsables de seguridad.	8
HU-06	Como administrador de sistemas, quiero que las	Alta	-Se definen políticas de corrección automática.	21

	vulnerabilidades críticas sean corregidas automáticamente para mejorar la seguridad del INS.		-Se implementan parches sin intervención manual. -Se documentan los cambios realizados.	
HU-07	Como líder de seguridad, quiero un dashboard con métricas en tiempo real para visualizar el estado de las vulnerabilidades	Media	-El dashboard muestra cantidad de vulnerabilidades. -Se visualiza el estado de las correcciones.	8

	en la infraestructura.		-Se permite la generación de reportes.	
HU-08	Como ingeniero DevOps, quiero integrar la automatización con un pipeline CI/CD para garantizar que las vulnerabilidades sean revisadas antes del despliegue.	Alta	-El pipeline CI/CD ejecuta escaneos de seguridad en cada despliegue. -Se bloquean despliegues inseguros. -Se generan reportes para revisión.	13
HU-09	Como analista de seguridad, quiero	Alta	-Se ejecutan pruebas de	8

	realizar pruebas de validación para garantizar que las correcciones no generen problemas en el sistema.		seguridad post-corrección. -Se documentan resultados y hallazgos. -Se ajustan configuraciones si es necesario.	
HU-10	Como gerente de TI, quiero que se realice una capacitación al equipo de seguridad sobre el nuevo modelo automatizado	Media	-Se diseña un plan de capacitación. -Se realizan sesiones de entrenamiento.	5

	para asegurar su correcto uso.		-Se genera material de referencia.	

Tabla 7

Casos de uso historias de usuario

ID	Nombre del caso de uso	Actor principal	Descripción	Precondiciones	Fujo principal	Flujo Alternativo	Postcondiciones
CU-01	Evaluar estado actual del proceso de detección de vulnerabilidades	Analista de seguridad.	El analista evalúa el proceso actual de detección de vulnerabilidades, identifica áreas de mejora, herramientas y	Acceso a herramientas de escaneo actuales y documentación de procesos.	1.Revisar herramientas actuales. 2.Analizar procesos actuales. 3.Identificar brechas de seguridad.	N/a	Se genera un informe con áreas de mejora y brechas de seguridad.

			brechas de seguridad.		4.Generar informe de diagnóstico.		
CU -02	Diseñar la arquitectura del modelo automatizado	Arquitecto de software	El arquitecto diseña la arquitectura del sistema para asegurar la integración con las herramientas existentes.	Requisitos de integración definidos.	1.Definir arquitectura escalable 2.Validar tecnologías compatibles. 3.Documentar la arquitectura.	N/A	Se obtiene la arquitectura definida y documentada.
CU -03	Integrar herramienta de escaneo de vulnerabilidades	Ingeniero DevOps	El ingeniero integra una herramienta de escaneo de	Herramienta seleccionada.	1.Configurar la herramienta de escaneo	Si la herramienta falla, se prueba una alternativa.	La herramienta está integrada correctamente y genera reportes

			vulnerabilidades para detectar amenazas automáticamente.		2.Ejecutar un escaneo de prueba 3.Verificar la integración con el sistema.		de vulnerabilidades.
CU-04	Automatizar ejecución de escaneos de vulnerabilidades	Desarrollador	El desarrollador automatiza los escaneos de vulnerabilidades para reducir intervención manual.	Acceso a sistema de automatización	1.Programar escaneos automáticos periódicos 2.Configurar generación de reportes automáticos 3.Integrar alertas para	Si la programación falla, se ajustan las configuraciones.	Los escaneos son automáticos y se generan reportes con alertas.

					vulnerabilidades críticas.		
CU-05	Recibir alertas en tiempo real para vulnerabilidades críticas.	Analista de seguridad	El analista recibe alertas en tiempo real cuando se detectan vulnerabilidades críticas para reaccionar rápidamente.	Sistema de alertas configurado.	1.Configurar alertas en SIEM 2.Configurar detalles de la vulnerabilidad en las alertas 3.Notificar a los responsables de seguridad.	Si la alerta no se genera correctamente, se revisa la configuración.	Se reciben alertas detalladas y notificaciones para corrección.
CU-06	Corregir vulnerabilidades críticas automáticamente.	Administrador de sistemas.	El administrador define y ejecuta políticas para corregir vulnerabilidades	Herramientas de corrección configuradas.	1.Definir políticas de corrección automática	Si no se corrige correctamente, se configuran las políticas.	Las vulnerabilidades críticas se corrigen automáticament

			críticas automáticamente.		2.Implementar parches de seguridad sin intervención manual 3.Documentar los cambios.		e y se documentan los cambios.
CU-07	Crear dashboard con métricas en tiempo real.	Líder de seguridad	El líder de seguridad solicita la visualización en tiempo real de métricas sobre vulnerabilidades.	Acceso a datos de vulnerabilidades.	1.Diseñar el dashboard con métricas de vulnerabilidades 2.Visualizar estado de las correcciones	Si los datos no se actualizan, se revisan las fuentes de información.	El dashboard muestra métricas en tiempo real y permite generar reportes.

					3.Permitir generación de reportes.		
CU -08	Integrar automatización en pipeline CI/CD	Ingeniero DevOps	El ingeniero integra la automatización de escaneos en el pipeline CI/CD para asegurar la revisión de vulnerabilidades antes del despliegue.	Pipeline CI/CD configurado.	1.Integrar escaneos de seguridad en cada despliegue 2.Bloquear despliegues inseguros 3.Generar reportes para revisión.	Si el despliegue es bloqueado se revisa el código.	Los escaneos de seguridad se ejecutan en cada despliegue y los reportes se generan.
CU -09	Realizar pruebas de validación post-corrección.	Analista de seguridad	El analista realiza pruebas para validar que	Corecciones implementadas	1.Ejecutar pruebas de seguridad	Si los resultados no son	Las pruebas son satisfactorias y

			las correcciones no generen nuevos problemas en el sistema.		2.Documentar resultados 3.Ajustar configuraciones si es necesario.	satisfactorios, se ajustan las correcciones.	se documentan los resultados.
CU-10	Capacitar al equipo de seguridad	Gerente de TI	El gerente organiza una capacitación para el equipo de seguridad sobre el nuevo modelo automatizado.	Plan de capacitación definido.	1.Diseñar el plan de capacitación 2.Realizar sesiones de entrenamiento 3.Generar material de referencia.	Si no se cumplen los objetivos, se ajustan los contenidos	El equipo de seguridad está capacitado y tiene material de referencia.

6.4 Arquitectura de la solución

De acuerdo con la investigación realizada y basado en las condiciones y posibilidades actuales del INS, se determina que la automatización más probable de implementar en el transcurso de este proyecto es la de la aplicación de parches de los servidores de plataforma Windows, mediante el Azure Update Manager, esto debido a que el INS ya cuenta con la suscripción respectiva y la plataforma de servidores es virtual en un 95 %. Por este motivo se presentan las dos opciones de arquitectura de solución, en primer lugar, la configuración del Azure Update Manager y su aplicación en la plataforma de servidores y en segundo lugar la arquitectura que implicaría la automatización general del proceso.

6.4.1. Diseño de la solución de automatización del parchado en los servidores virtuales

Los pasos para configurar el Azure Update Manager son los siguientes:

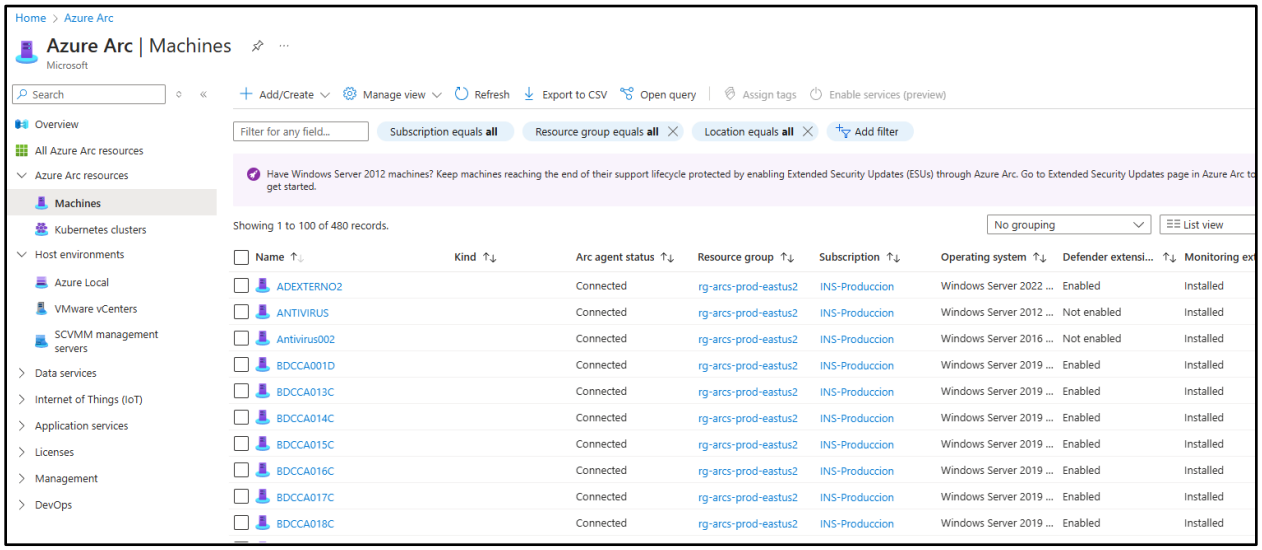
1. Accesar al portal de Azure
2. Navegar hasta Azure Update Manager
3. Seleccionar Suscripción y Grupo de Recursos
4. Configurar la Política de Actualización.
5. Asignar a Máquinas Virtuales o Grupos.
6. Monitoreo y Cumplimiento.

Luego de configurar al AUM (Azure Update Manager), se debe instalar en los servidores el agente del Azure Arc, esta herramienta permite la integración con la plataforma del Update Manager de forma nativa, y facilita la configuración de la aplicación de parches en esta plataforma.

Los servidores deben aparecer en estado Conectados en la consola de Azure Arc para que esta aplicación sea efectiva:

Figura 50

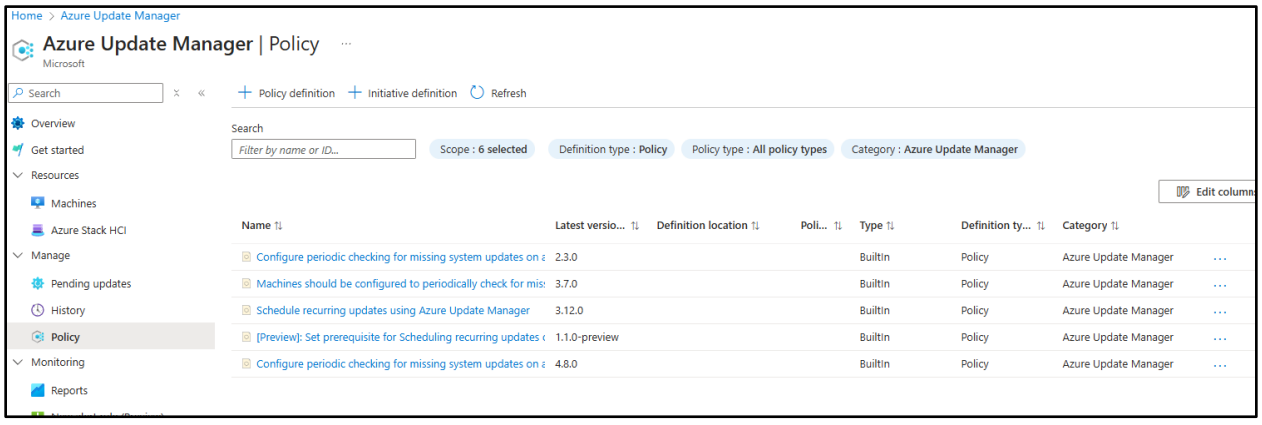
Consola de Azure Arc en INS



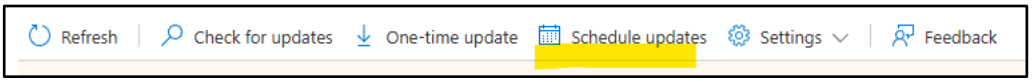
Luego de esto se define la política que se debe aplicar en los equipos:

Figura 51

Políticas de aplicación de parches



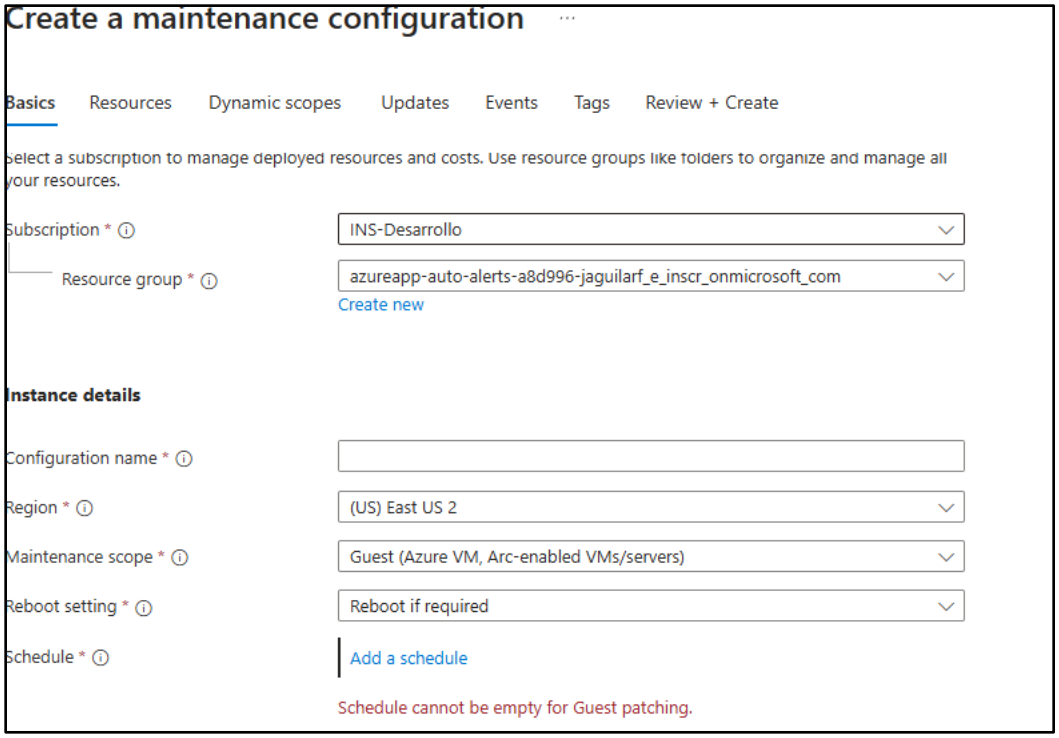
Posteriormente se agendan los updates, mediante la opción respectiva:



Acá se deben seleccionar varios parámetros, por ejemplo, la suscripción, el grupo de recursos, un nombre de la tarea, la Región, la necesidad de reiniciar si es el caso y finalmente la fecha y hora de la aplicación de los parches, como se ve en la siguiente imagen:

Figura 52

Configuración de la tarea de parchado



Finalmente se realiza el monitoreo de la tarea y la revisión de los reportes finales para verificar cualquier posible problema o corrección que se deba hacer en ese momento.

En una primera etapa se estarán incluyendo los servidores del ambiente de desarrollo con el fin de realizar las pruebas respectivas sin causar interrupción en los servicios, la aplicación de parches se realizará de forma mensual, el tercer sábado de cada mes. Luego de cada aplicación se revisarán las bitácoras de errores y se harán las correcciones del caso, esto con el fin de tener la configuración afinada cuando se deba aplicar en los servidores de producción.

6.4.2. Diseño de la herramienta de automatización de corrección de vulnerabilidades

A continuación, se explica el diseño de la arquitectura que debe llevar la solución final de automatización del proceso de corrección de vulnerabilidades, cabe destacar que este diseño aplica para cualquiera de las herramientas que sean utilizadas y que se tiene como base que la detección o el escaneo de la infraestructura se realiza por medio del software llamado Nessus.

Esta arquitectura debe ser modular y escalable con el fin de que se puedan cubrir todos los aspectos de la seguridad involucrados en el proceso. En este sentido la arquitectura diseñada es la siguiente:

6.4.2.1. Capas principales de la Arquitectura:

- Capa de percepción o detección de vulnerabilidades (Nessus)
- Capa de decisión (Análisis y priorización, se realiza actualmente de forma manual y con la ayuda del tablero Kanban)
- Capa de Ejecución (Corrección de vulnerabilidades, se realiza de forma manual)
- Capa de Monitoreo y Retroalimentación (Validación y mejora continua)

6.4.2.2. Flujo del Proceso

El flujo del proceso debe ser continuo y además automático para asegurar una rápida respuesta ante nuevas amenazas que puedan surgir:

A. Detección de Vulnerabilidades

A1. Herramientas de escaneo

- Se utiliza la herramienta Nessus
- El escaneo de las vulnerabilidades se realiza de forma mensual, sin embargo, es posible realizar escaneos adicionales en caso de ser necesario.

A2. Integración con el CI/CD (Integración/Desarrollo continuo)

- Si el entorno es dinámico se debe integrar la herramienta Nessus con las herramientas de vulnerabilidades en el pipeline CI/CD.
- Cuando se despliega una nueva versión, el sistema es capaz de verificar vulnerabilidades automáticamente.

A3. Integración con el entorno hibrido

- Realizar la integración mediante el Azure Arc con los servidores actuales con el fin de detectar vulnerabilidades de forma periódica.

A4. Sistemas de monitoreo y detección en tiempo real:

- Se deben implementar herramientas de detección de intrusiones (IDS) adicionales a los ya existentes en la institución, con el fin de detectar comportamientos inusuales y posibles vulnerabilidades en tiempo real.

B. Análisis y Priorización de Vulnerabilidades

B1. Centralización de alertas:

- Se utilizará un sistema centralizado como SIEM, que permita almacenar y correlacionar alertas generadas por las herramientas de escaneo y otros sistemas de seguridad.

B2. Clasificación y Priorización:

- Se implementará una política de priorización de vulnerabilidades, por ejemplo, la CVSS (Common Vulnerability Scoring System), para clasificar las vulnerabilidades de acuerdo con su criticidad y el impacto potencial.

- Las vulnerabilidades se deben evaluar en función de los riesgos específicos para la organización, basado en los parámetros existentes y la clasificación de sistemas críticos realizada por la Unidad de Continuidad del Negocio (UCN).

B3. Flujos de Trabajo Automatizados:

- Se implementará una herramienta de orquestación como Ansible, Chef, Puppet o SaltStack, esto permitirá automatizar la evaluación y gestión de vulnerabilidades, si una vulnerabilidad tiene un parche disponible, el sistema podría automáticamente activar un flujo de trabajo para corregirla o en su defecto se podría configurar esta aplicación de parche en el Azure Update Manager.

C. Corrección de Vulnerabilidades

C1. Automatización de parches

- La automatización de parches se realizará por medio de la herramienta Azure Update Manager

C2. Gestión de configuración y remediación:

- Por medio de las herramientas de gestión de configuración como Ansible, Puppet o Terraform, se automatizará la corrección de configuraciones incorrectas que podrían generar vulnerabilidades.

C3. Automatización de respuesta a incidentes (SOAR):

- Las plataformas SOAR pueden automatizar las respuestas ante incidentes y apoyar el proceso ya existente, lo que permite que las vulnerabilidades críticas se mitiguen rápidamente sin intervención manual.

D. Monitoreo Continuo y Retroalimentación

D1. Monitoreo Post-Corrección:

- Luego de aplicar los parches o de realizar correcciones, se deben realizar escaneos de validación, esto permitirá asegurar que las vulnerabilidades han sido realmente solucionadas.
- Con el uso de herramientas como Qualys, OpenVAS, o servicios de escaneo en la nube se podrá implementar un monitoreo continuo.

D2. Retroalimentación y mejora continua:

- Se establecerán ciclos de retroalimentación donde los resultados de las evaluaciones de vulnerabilidades alimenten nuevas estrategias de detección y corrección, esto a cargo del equipo Chirripó y del área de Seguridad de TI.
- Se implementará el ciclo Plan-Do-Check-Act (PDCA) para asegurar que las vulnerabilidades detectadas sean gestionadas de forma continua.

D3. Integración con Herramientas de Gestión de Incidentes:

- Se integrará la herramienta con el software de gestión de incidentes vigente en la institución en el momento de la implementación.

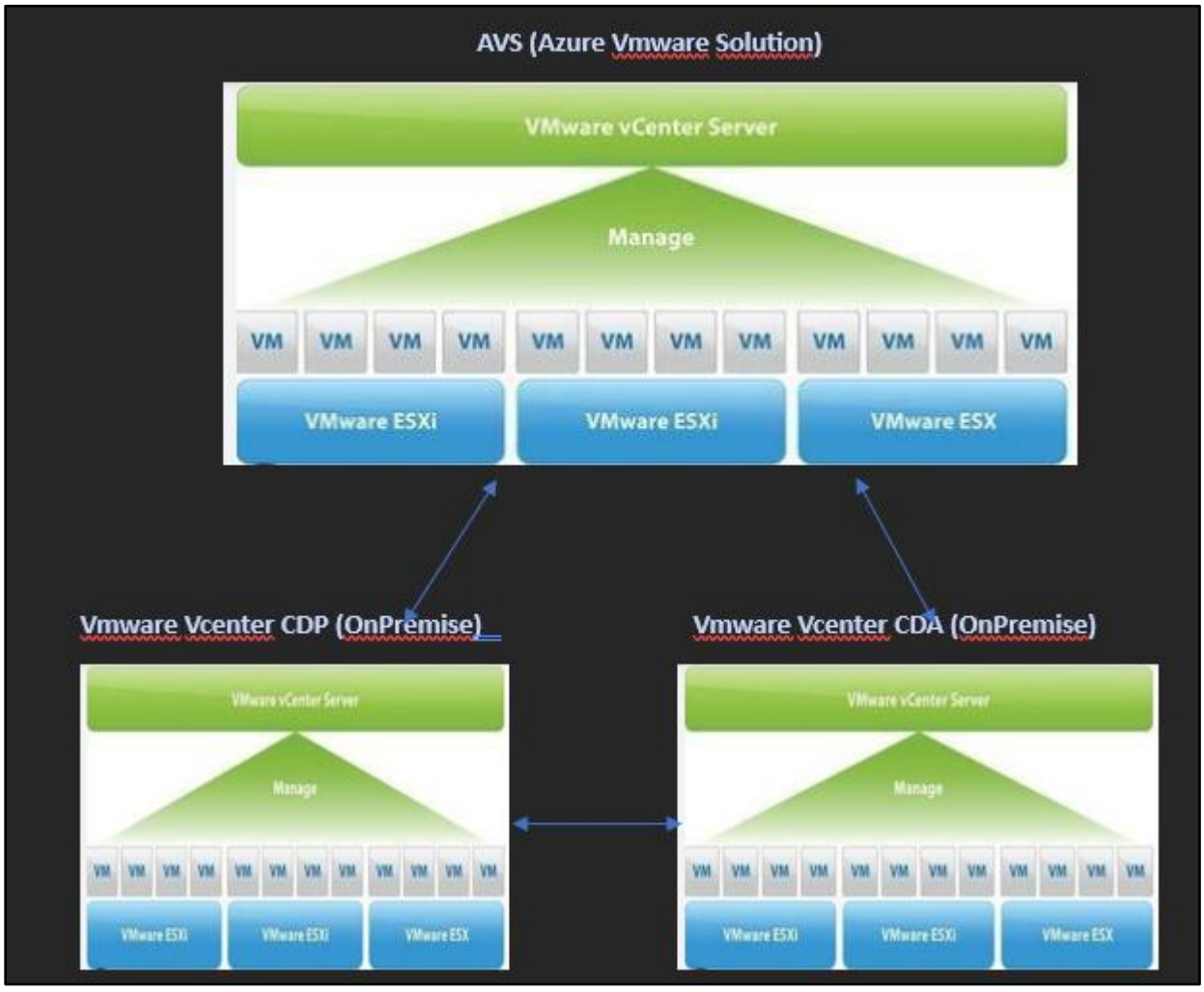
Figura 53

Diagrama Conceptual de la Arquitectura de automatización

Infraestructura actual del INS

Figura 54

Infraestructura actual del INS



La infraestructura actual de servidores del INS de acuerdo con lo que se puede ver en la imagen está definida de la siguiente manera:

- Vcenter en azure por medio de la solución AVS (Azure Vmware Solution) un total de 423 servidores, ambientes de desarrollo y producción.

- Vcenter On Premise Centro de Datos Principal (CDP), un total de 125 servidores ambientes de desarrollo y producción.
- Vcenter On Premise Centro de Datos Alterno (CDA), un total de 56 servidores ambientes de desarrollo y producción.

Sistemas operativos

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Red Hat Linux 9.4
- CentOS-7.9

6.5 Metodología de la implementación

Para garantizar una implementación efectiva, se utilizará un enfoque basado en metodologías ágiles, específicamente Scrum, con iteraciones de dos semanas para la entrega de incrementos funcionales. Las fases del proceso incluyen:

1. Fase de planificación:
    - Definición de objetos específicos y alcance del modelo automatizado.
    - Identificación de herramientas y tecnologías necesarias.
    - Asignación de roles y responsabilidades en el equipo de implementación.

2. Fase de desarrollo e integración:
    - Configuración de herramientas de escaneo y análisis de vulnerabilidades.
    - Desarrollo de flujos automatizados de corrección utilizando Ansible, Puppet o Chef.
    - Implementación de dashboards en SIEM y herramientas de monitoreo como Grafana o Power BI.
3. Fase de pruebas y validación:
    - Pruebas de detección de vulnerabilidades en entornos de prueba y producción.
    - Evaluación del impacto de las automatizaciones en la seguridad del sistema
    - Ajustes y optimización según los resultados obtenidos.
4. Fase de implementación y despliegue:
    - Despliegue gradual en los entornos productivos
    - Monitoreo continuo del rendimiento y efectividad del modelo.
    - Capacitación del personal en la administración del sistema.
5. Fase de mantenimiento y mejora continua:
    - Evaluaciones periódicas para optimizar la detección y mitigación de vulnerabilidades.
    - Actualización de reglas y configuraciones en función de nuevas amenazas.
    - Integración con futuras tecnologías para mejorar la eficiencia del modelo.

6.6 Evaluación y validación del modelo

Para validar la efectividad del modelo se definen:

- Pruebas de rendimiento en un entorno controlado

- Simulaciones de ataques para evaluar la capacidad de detección y corrección
- Comparación con métricas previas para medir mejoras en tiempos de respuesta y reducción de vulnerabilidades.

2.Creación del producto backlog

El Product Owner define los requerimientos principales, priorizando funcionalidades clave como:

1. Análisis de la situación actual de seguridad
2. Integración con herramientas de escaneo de vulnerabilidades (Ej.Nessus, Open VAS).
3. Desarrollo de scripts de automatización.
4. Implementación de CI/CD para el despliegue continuo.
5. Pruebas y validaciones de seguridad.
6. Capacitación del equipo del INS.

3.Priorización y planificación de sprints

Cada sprint tiene una duración de 2 semanas, y se organizan en función de la prioridad del backlog:

3.1.Sprint 1: análisis y diagnóstico

- Evaluación de procesos actuales de detección de vulnerabilidades.
- Identificación de herramientas a integrar.
- Documentación inicial del proyecto.

3.2.Sprint 2: Diseño del modelo automatizado

- Creación de arquitectura del sistema
- Selección de tecnologías y herramientas

- Definición de estándares de seguridad a cumplir

3.3.Sprint 3-4: desarrollo e integración

- Desarrollo de scripts y automatización.
- Integración con herramientas de análisis de vulnerabilidades.
- Implementación de CI/CD para despliegue automático.

3.4.Sprint 5: pruebas y validación

- Pruebas funcionales y de seguridad.
- Ajustes según retroalimentación
- Documentación final del sistema

3.5.Despliegue y capacitación

- Implementación en el entorno productivo del INS
- Capacitación a los equipos internos
- Monitoreo y mejoras continuas

4. Reuniones Scrum

- Dayli stand-ups: revisión rápida del avance diario y obstáculos
- Sprint planning: definición de tareas en cada sprint.
- Sprint review: presentación de avances y validación con stakeholders.
- Sprint retrospective: evaluación de mejoras en la metodología.

6.7 Manual de implementación

Este manual proporciona las directrices para la rápida integración del modelo de automatización en la infraestructura tecnológica del INS.

6.7.1 Preparación del entorno

1. Ejecución de escaneo mediante herramienta Nessus.

2. Revisión de resultados obtenidos de los escaneos.

3. Organización de las tarjetas, de acuerdo con el grado de criticidad de los sistemas y el tipo de vulnerabilidad encontrada.

6.7.2 Configuración del sistema de automatización de aplicación de parches

1. Instalación del agente de Azure Arc en los equipos respectivos.

2. Creación de política para la instalación de parches en Azure Update Manager en los servidores seleccionados.

3. Definición de reglas de revisión de aplicación de parches para revisión posterior a la ejecución del proceso.

6.7.3 Integración y monitoreo

1. Configurar notificaciones tras la ejecución del proceso para los administradores.

2. Brindar acceso a los dashboard de Azure a los administradores para su respectiva revisión.

3. Configuración de integración con el software de monitoreo existente en la institución (Vityl).

6.7.4 Pruebas y validación

1. Ejecución de la aplicación de parches en los servidores del ambiente de desarrollo, como parte de la prueba para validar la efectividad del modelo.

2. Revisión manual de la aplicación correcta de parches de acuerdo con la configuración.

3.Ajuste de parámetros y optimización del sistema basado en resultados de prueba.

6.8 Manual de procedimientos de automatización

Este manual establece los procedimientos de automatización basados en las normas ISO 27001 y NIST 2, asegurando la correcta implementación y gestión de la seguridad de la información en el INS.

6.8.1 Procedimientos generales

- Definición de políticas de seguridad y roles de acceso
- Implementación de controles de auditoría y monitoreo
- Evaluación de riesgos y aplicación de medidas correctivas.

6.8.2 Configuración de herramientas de automatización

- Instalación y configuración de herramientas como Ansible, Puppet y Chef.
- Creación de scripts y playbooks para la mitigación de vulnerabilidades.
- Integración con sistemas SIEM y plataformas de gestión de logs.

6.8.3 Procedimiento de respuesta a vulnerabilidades

- Escaneo programado y análisis de vulnerabilidades.
- Evaluación de criticidad y generación de reportes automáticos.
- Aplicación de correcciones y validación de seguridad post-implementación.

6.8.4 Mantenimiento y mejora continua

- Monitoreo constante y actualización de herramientas de automatización.
- Implementación de parches de seguridad y revisión de configuraciones.
- Revisión periódica de cumplimiento normativo y mejores prácticas.

6.9 Plan de capacitación

Para garantizar una óptima implementación del modelo automatizado, se diseñará un plan de capacitación dirigido al personal del INS. Este plan abordará los siguientes aspectos clave:

6.9.1 Público objetivo

- Personal de Operaciones y Soporte Técnico.
- Equipos de Seguridad de la Información.
- Administradores de sistemas.
- Responsables de cumplimiento normativo.

6.9.2 Objetivos del plan de capacitación

1.Familiarizar al personal con el modelo automatizado y sus componentes.

2.Capacitar en la ejecución de escaneos de vulnerabilidades y análisis de resultados.

3.Entrenar en la aplicación de parches y mitigaciones automatizadas.

4.Instruir sobre la gestión y monitoreo de la plataforma de seguridad.

5.Brindar conocimientos sobre buenas prácticas en ciberseguridad y cumplimiento normativo.

6.9.3 Temas de capacitación

1.Introducción al modelo automatizado

- Arquitectura y componentes clave.
- Beneficios y objetivos de la implementación.

2.Ejecutando escaneos de vulnerabilidades

- Configuración y uso de Nessus.
- Interpretación de reportes y análisis de criticidad.

3.Automatización de corrección de vulnerabilidades

- Uso de Ansible, Puppet y Chef.
- Creación y gestión de playbooks para parches de seguridad.

4.Monitoreo y respuesta a incidentes

- Integración con SIEMs (Splunk, ELK Stack)
- Configuración de alertas y generación de reportes.

5.Buenas prácticas en ciberseguridad

- Estrategias de gestión de vulnerabilidades
- Cumplimiento de estándares ISO 27001, NIST y CIS Controls.

6.Simulaciones y ejercicios prácticos

- Simulación de ataques y respuesta automatizada.
- Evaluación de tiempos de respuesta y efectividad del modelo.

6.9.4 Metodología de capacitación

- **Sesiones teóricas y prácticas**: Explicaciones detalladas seguidas de ejercicios prácticos.
- **Capacitación en línea y presencial**: Material disponible en formato digital y talleres presenciales.
- **Pruebas de conocimiento**: Evaluaciones periódicas para medir la comprensión de los temas.
- **Manuales y guías**: Documentación de referencia para consulta posterior.

6.9.5 Evaluación y seguimiento

Para garantizar la efectividad de la capacitación, se implementará un sistema de evaluación y seguimiento que incluirá:

Encuestas de retroalimentación después de cada sesión.

- Evaluaciones prácticas para medir el desempeño del personal.
- Revisión de métricas de implementación y adopción del modelo automatizado.
- Sesiones de actualización periódicas para reforzar conocimientos y adaptarse a nuevas amenazas y tecnologías.

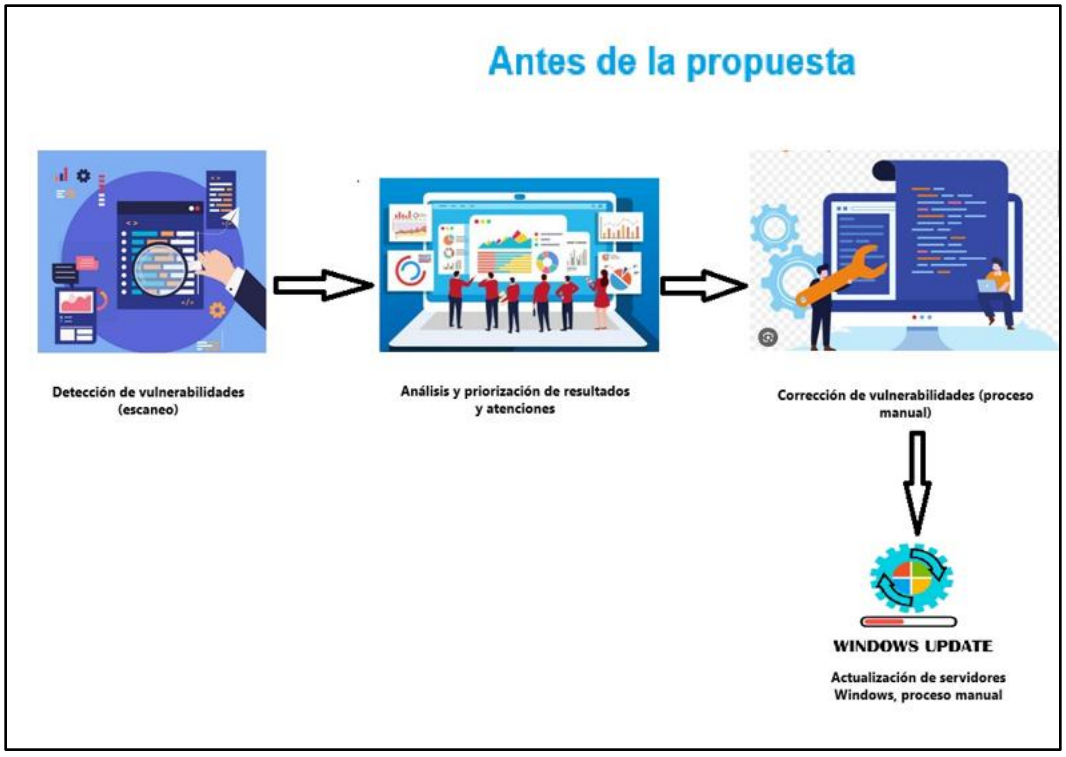
6.10. Diagramas y Manuales

En esta sección se presentan los diagramas y manuales que fundamentan todo lo explicado en los puntos anteriores.

6.10.1. Diagrama del proceso antes de la propuesta de este proyecto

Figura 55

Diagrama antes de la propuesta



Nota. Fuente: Diseño propio.

El proceso actual consta de 3 fases:

1. Detección (escaneo) de vulnerabilidades: este proceso ya está automatizado y se realiza por medio de la herramienta Nessus, el ismo es ejecutado por el departamento de Seguridad de TI cada mes. Cantidad de recursos 2 personas.

2. Análisis de resultados y priorización de atenciones: este proceso se alimenta del escaneo, los resultados son analizados y organizados por medio de un tablero Kanban en el cual se priorizan las atenciones de acuerdo con el nivel y tipo de vulnerabilidad, así como la criticidad del servidor

respectivo, este proceso es actualmente manual y es realizado por miembros del departamento de Seguridad de TI, así como miembros del equipo Chirripó, así como personal de la Dirección de TI y la jefatura del departamento de OST. Cantidad de recursos 12.

3. Corrección de vulnerabilidades y parchado de servidores: la corrección de las vulnerabilidades se realiza de forma manual en sesiones semanales que se realizan dos veces, siempre y cuando no se vean afectados servicios críticos, en caso de que así sea se debe coordinar la ventana de mantenimiento respectiva. Cantidad de recursos 6 personas.

El parchado de servidores también es un proceso manual que es realizado mensualmente, los viernes en la noche para el ambiente de desarrollo y los sábados y domingos para el ambiente productivo. Cantidad de recursos 5. En total participan 11 personas en la corrección. Se cancela un monto de ₡1.000.000 mensual por concepto de horas extras y se utilizan al menos 10 horas mensuales en estas labores.

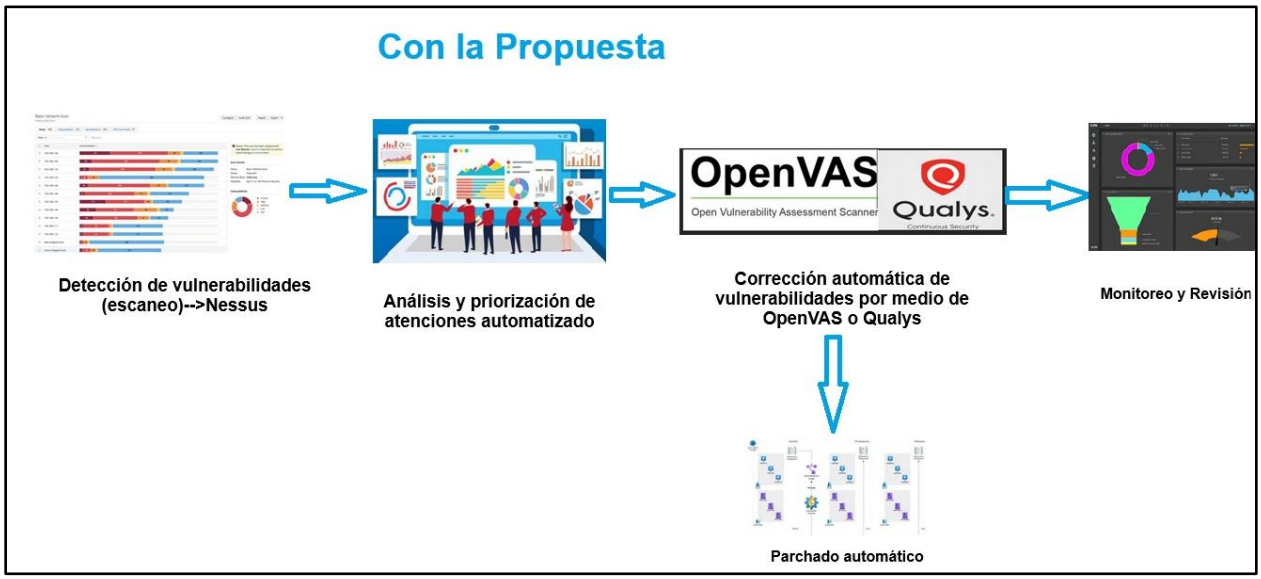
Es importante destacar que en las sesiones se lleva además el seguimiento de la atención de las tarjetas respectivas, sin que haya un proceso específico para esta labor.

Cantidad total de recursos que participan del proceso 25 personas.

6.10.2. Diagrama con la propuesta de este proyecto

Figura56

Diagrama con la propuesta



Nota. Fuente: Diseño propio

La propuesta contempla 4 fases del proceso:

1. Detección (escaneo) de vulnerabilidades: este proceso ya está automatizado y se realiza por medio de la herramienta Nessus, el ismo es ejecutado por el departamento de Seguridad de TI cada mes. Cantidad de recursos 2 personas.

2. Análisis y priorización de atenciones: luego de realizado el escaneo por medio de la herramienta Nessus se realiza el análisis y la priorización de las vulnerabilidades, utilizando las herramientas OpenVas y Qualys que serán configuradas de acuerdo con los parámetros establecidos de criticidad e importancia de las aplicaciones respectivas y siempre buscando no tener interrupciones en los servicios. Cantidad de recursos necesarios 6 personas.

3. Corrección de vulnerabilidades: por medio de las herramientas Ansible o Puppet, se realizarán las configuraciones respectivas que permitan ejecutar correcciones de forma automática

respetando los criterios internos de criticidad y no interrupción de servicios, luego de cada ejecución se hará una revisión manual. Cantidad de recursos necesarios 3 personas.

Para el parchado automático se utilizará la herramienta llamada Azure Update Manager, que permitirá la aplicación de parches de forma automática cada mes, mejorando el proceso actual y disminuyendo la cantidad de recurso humano necesario. Cantidad de recursos necesarios 2.

Con esta propuesta se estará reduciendo el costo de pago de horas extras a solamente ₡225.000 por mes, esto representa un ahorro importante, además se necesitarán solamente 6 horas mensuales en todo el proceso, esto permite que los funcionarios puedan emplear este tiempo en funciones adicionales.

4. Monitoreo y Seguimiento: Se realizará una integración de la herramienta elegida (OpenVAS, Qualys) con Azure y el software vigente de gestión de incidentes con el fin de mantener un monitoreo claro de la aplicación de correcciones, así como de la aparición de nuevas vulnerabilidades en tiempo real. Cantidad de recursos 3 personas.

Cantidad total de recursos que participan en el proceso 10 personas.

6.10.2. Diagramas de la configuración del Azure Update Manager

A continuación, se presentan imágenes propias del proceso de configuración realizado en Azure Update Manager.

Figura 57

Tablero Principal

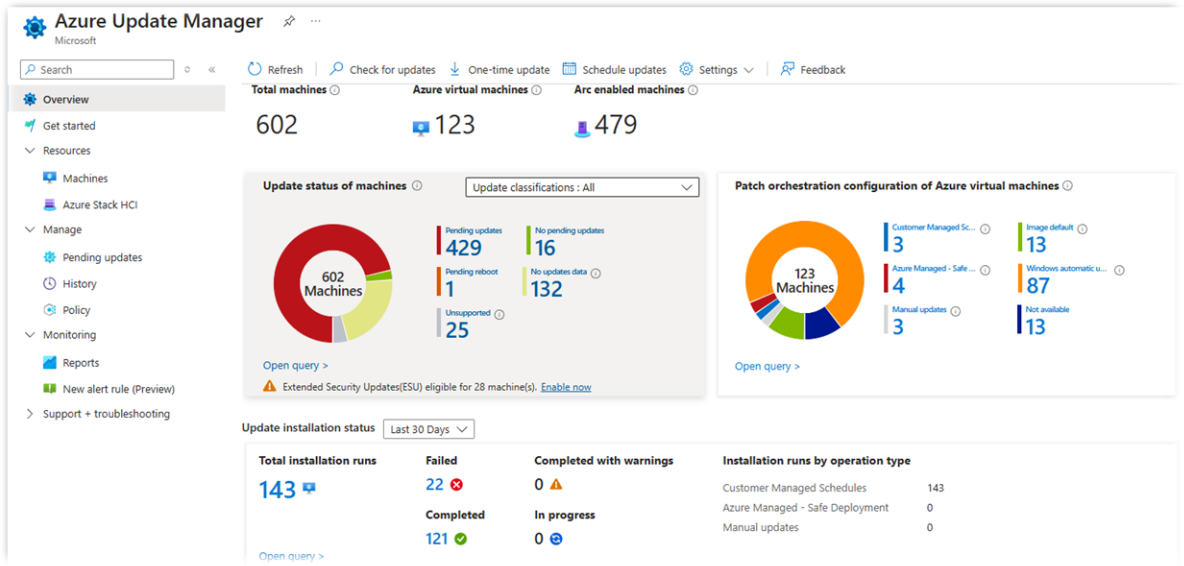


Figura 58

Diagrama de actualizaciones pendientes.

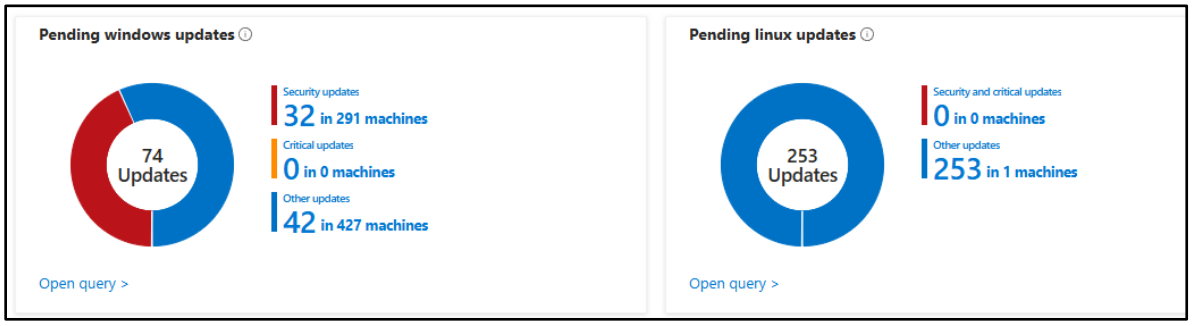


Figura 59

Máquinas configuradas

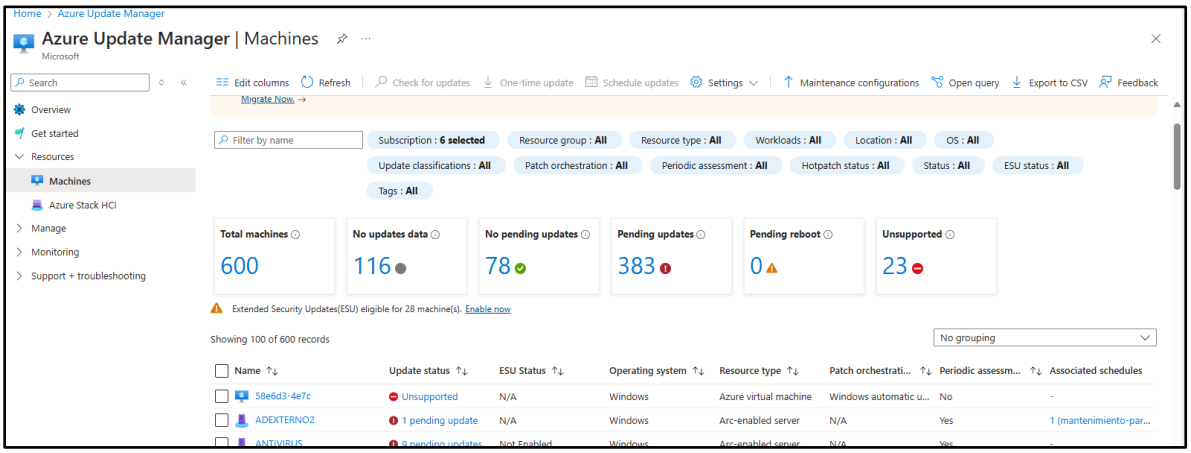
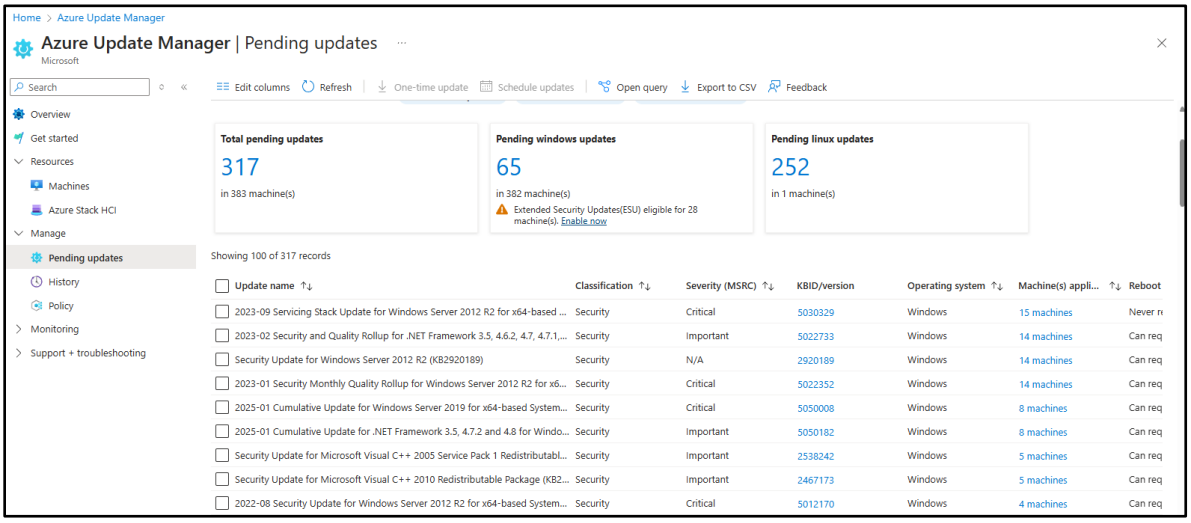


Figura 60

Actualizaciones pendientes



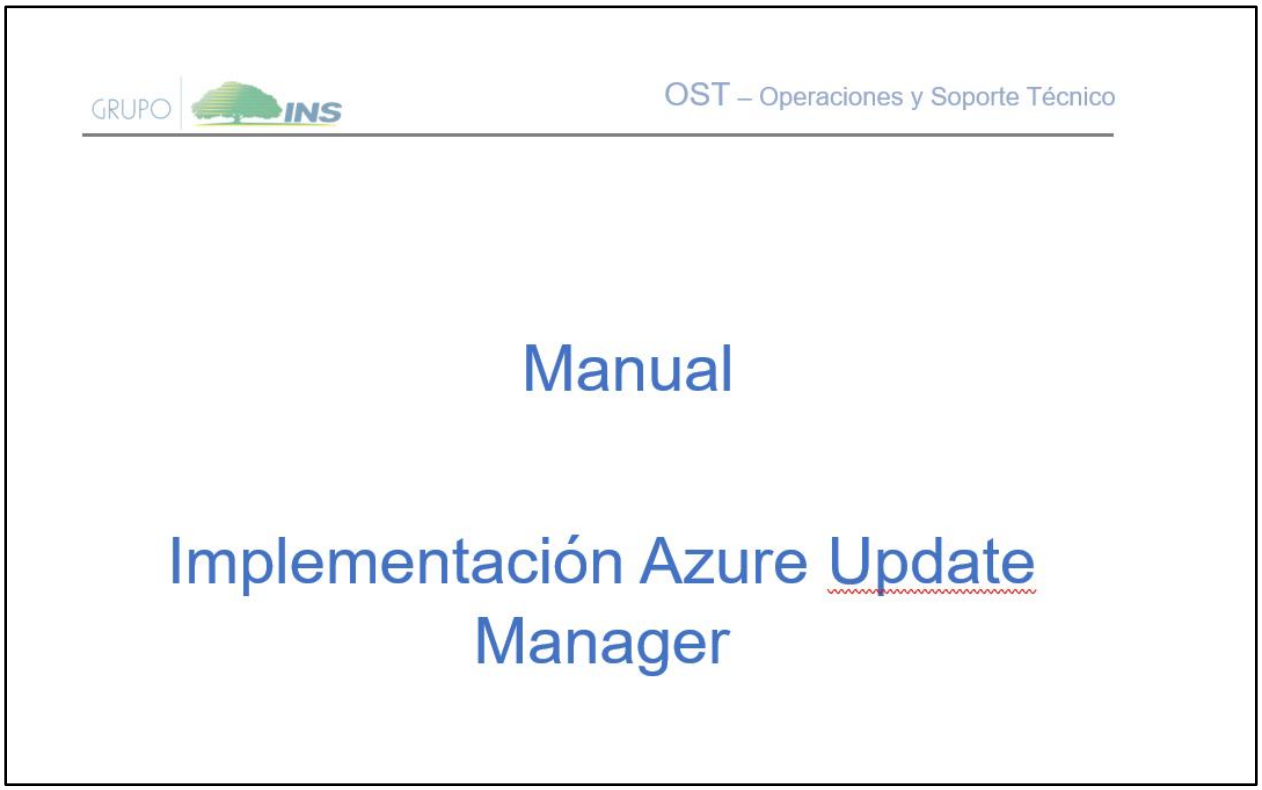
6.10.3. Concientización al personal interno

Debido a que el eslabón más débil en la cadena de protección de los equipos tecnológicos sigue siendo el usuario final, se estará realizando periódicamente una campaña de concientización al personal con mensajes como los siguientes:

Figura 61

Avisos personal INS

6.10.4. Manual de implementación de Azure Update Manager



El objetivo de este manual es explicar el proceso de configuración de la herramienta Azure Update Manager, que permite realizar la aplicación automática de las actualizaciones de Windows en los servidores de la plataforma virtual institucional.

Los pasos para la configuración de esta herramienta son los siguientes:

1. En el Active Directory

1.1. Se debe crear una política en el AD que permite instalar en cada servidor que es registrado el agente de Azure Arc, que es clave para hacer la configuración de las actualizaciones automáticas.

GPO_Instalacion_AzureARC_Inmediato

1.1 Se debe crear una política que modifica el REGEDIT de los equipos para que busque las actualizaciones en los servers WSUS. Esta política además permite que las actualizaciones sean descargadas y se generen las notificaciones de las actualizaciones disponibles.

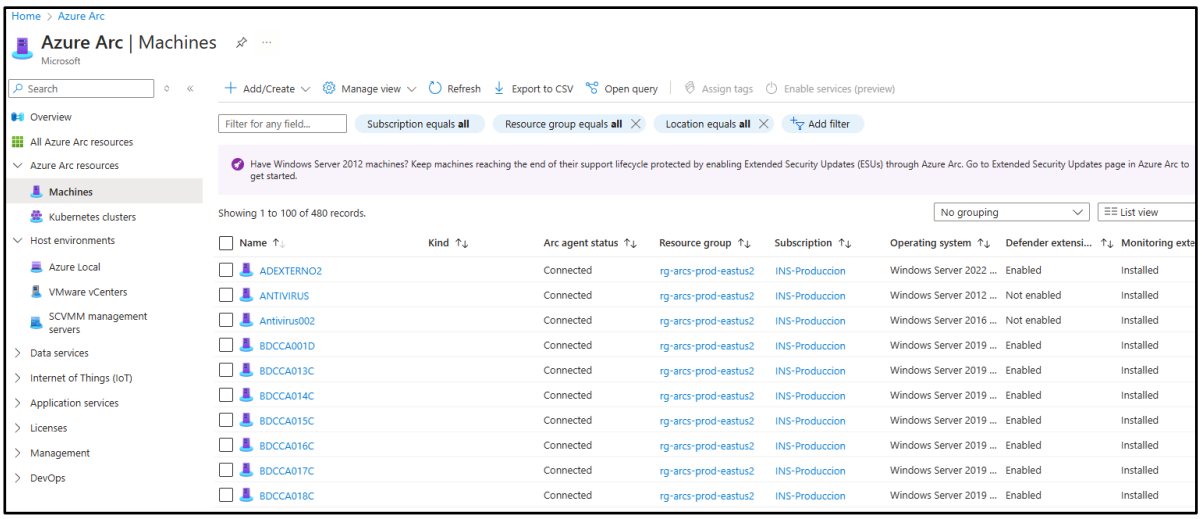
1.2. Se deben crear 3 servidores con el feature de WSUS para que sean los encargados de desplegar las actualizaciones hacia toda la infraestructura, estos servidores se crean en los 3 ambientes de interés, a saber:

- Azure
- AVS (Azure Vmware Solutions)
- On Premise

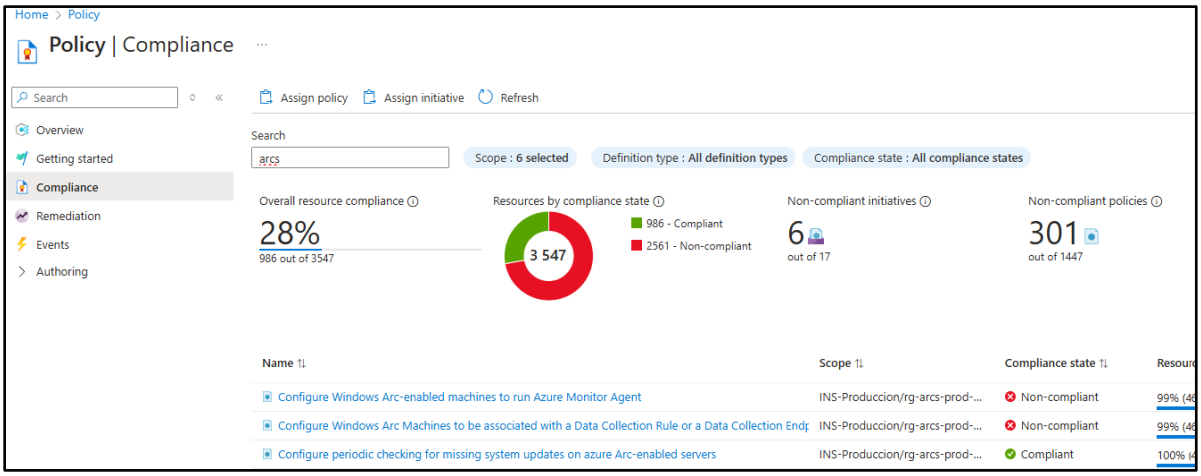
2. En Azure:

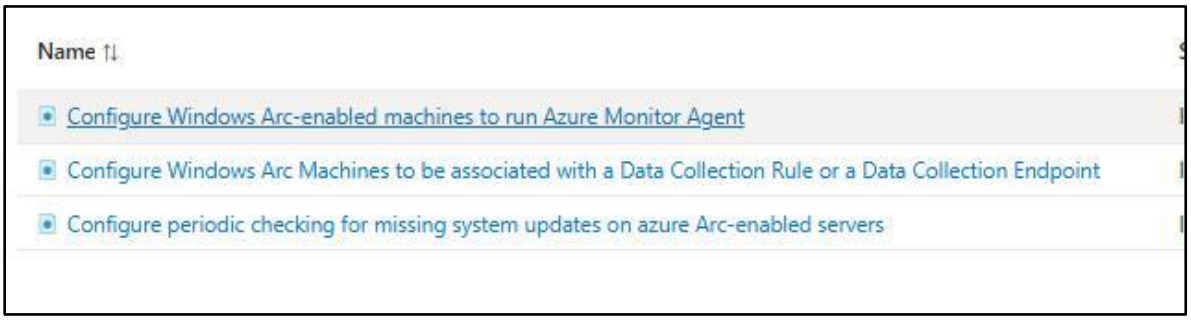
Los pasos necesarios para la configuración de la herramienta en el portal de Azure son los siguientes:

2.1. Las máquinas deben tener el agente de Azure Arc instalado.

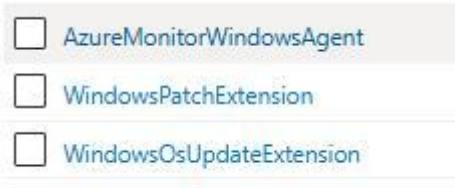


2.2. Por medio del Update Manager, se deben instalar 3 extensiones, estas se instalan por medio de las políticas de Azure (Policy).





Las 3 extensiones son las siguientes:



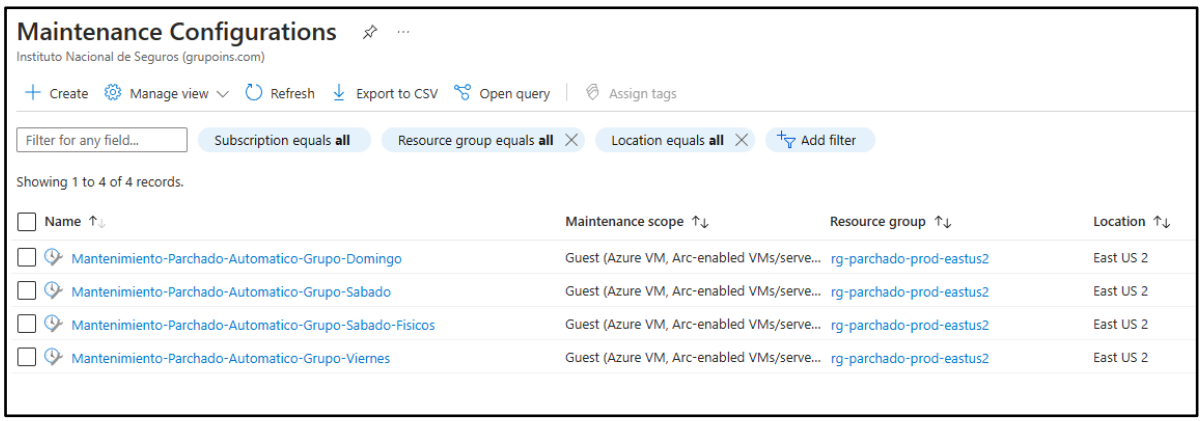
AzureMonitorWindowsAgent: envía información a un data collection que transmite la información a un log analytics y el SOC utiliza esa información para monitoreo preventivo.

WindowsPatchExtension: se instala automáticamente cuando el sistema realiza un assesment automático.

WindowsOSUpdateExtension: se instala automáticamente cuando el sistema realiza un assesment automático.

3. Maintenance Configurations:

Este es el paso final para configurar la instalación de las actualizaciones:

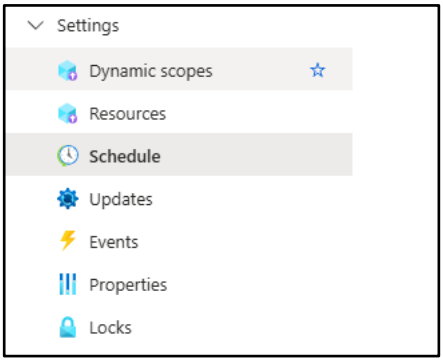


Se crean los grupos o planes de mantenimiento de acuerdo con las necesidades de la organización y la criticidad de los servidores, a saber:

- Parchado automático grupo Domingo: son los servidores cuyos sistemas solamente permiten que se puedan aplicar las actualizaciones este día.

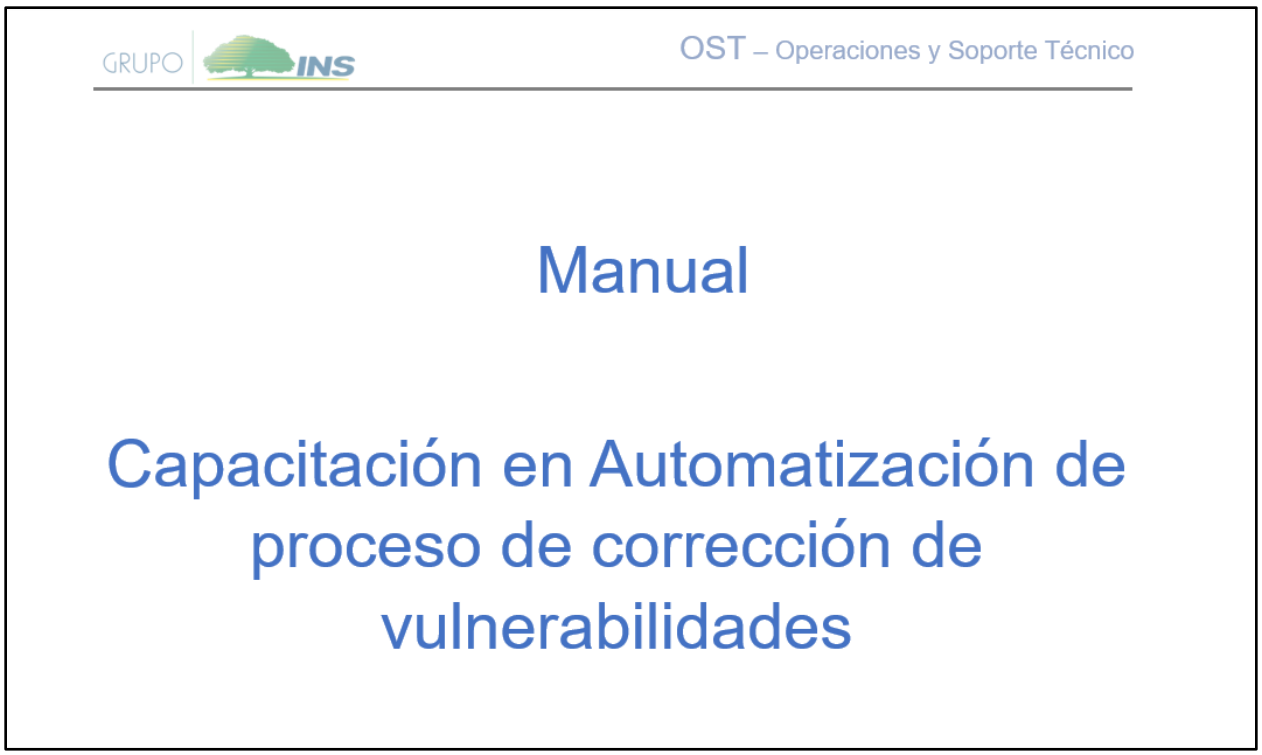
- Parchado automático grupo sábado: esta tarea se aplicará a los servidores del ambiente productivo.
- Parchado automático grupo sábado físicos: para servidores físicos que tengan instalado el agente de ARC.
- Parchado automático grupo viernes: en esta tarea se agregan los servidores del ambiente de desarrollo que se estarán actualizando viernes por la noche.

Las opciones de configuración son las siguientes:



Finalmente, luego de la configuración de la tarea y su respectiva ejecución se debe hacer una revisión manual en busca de posibles errores y correcciones o ajustes que se puedan aplicar.

6.10.4. Plan Capacitación



Objetivo

Este documento tiene como objetivo brindar una guía respecto al proceso de capacitación necesario para el personal del INS en el proceso de automatización en la detección y corrección de vulnerabilidades.

Paso 1: Capacitación personal

El primer paso del proceso consiste en realizar una capacitación del personal del departamento de Operaciones y Soporte Técnico, en la configuración y utilización del Azure Update Manager, así como en la revisión y seguimiento de la aplicación automática de los parches en los servidores configurados.

Paso 2: Capacitación a personal de Seguridad de TI:

La segunda etapa de la capacitación está dirigida al personal de Seguridad de TI, así como de OST, quienes estarán a cargo de la instalación, configuración, aplicación y seguimiento de la herramienta seleccionada para automatizar la corrección de vulnerabilidades, este proceso incluye, además, las pruebas respectivas.

Paso 3: Capacitación personal de monitoreo:

La tercera etapa es la capacitación al personal de monitoreo, pues parte del proceso consiste en integrar la herramienta seleccionada para la corrección de vulnerabilidades automáticas con la herramienta de monitoreo, con el fin de obtener los datos que permiten verificar no solo la correcta aplicación de estos sino prevenir posibles presencias de vulnerabilidades en tiempo real.

6.10.5. Pruebas de implementación

Se realizarán dos tipos de pruebas de implementación: las de la configuración del Azure Update Manager y aplicación de parches de forma automática y las de la herramienta de corrección de vulnerabilidades de forma automática.

Azure Update Manager: se configura la herramienta y se aplica la política en los servidores del ambiente de desarrollo y se valorará el resultado con el fin de realizar los ajustes respectivos.

Luego de esto se realiza una segunda ejecución y se repite el proceso hasta tenerlo completamente depurado, finalmente se realiza una tercera ejecución y se da el visto bueno para la puesta en producción.

Herramienta seleccionada aplicación de correcciones automáticas (OpenVAS, Qualys): los pasos necesarios para la ejecución de pruebas son las siguientes:

a.) Se realizan las configuraciones e integraciones necesarias, con las diferentes herramientas.

b.) Se configuran los servidores del ambiente de desarrollo para hacer la primera ejecución de correcciones automáticas.

c.) Se revisan los resultados y se hacen los ajustes respectivos.

Luego de esto se realiza la primera ejecución y se verifica el proceso, en busca de realizar cambios o ajustes en la configuración, luego de esto se realiza la segunda ejecución con su respectiva aplicación y finalmente una tercera ejecución antes de hacer la aplicación en producción.

Referencias Bibliográficas

Arias Buenaño, G., Merizalde Almeida, N. y Noriega García, N. (2013). *Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la informática y seguridad de la información de un medio de comunicación audio-visual*. https://dspace.ups.edu.ec/handle/123456789/5386

ARUBANETWORKS. (2024). *arubanetworks.com*. https://www.arubanetworks.com/es/faq/que-es-un-ngfw/

Atlassian. (2024). *atlassian.com*. https://www.atlassian.com/es/incident-management/incident-response/lifecycle#nist-incident-response-lifecycle

atlasti. (2023). *atlasti.com*. https://atlasti.com/es/guias/guia-investigacion-cualitativa-parte-1/investigacion-cualitativa

AVAST. (2022). *avast.com*. https://www.avast.com/es-es/c-sql-injection

AVSOFTWARE. (2023). *avsoftware.com*. https://www.avsoftware.com.mx/respuesta-a-incidentes-de-ciberseguridad-guia-de-nist/

aws. (2024). *aws.amazon.com*. Obtenido de aws.amazon.com: https://aws.amazon.com/es/what-is/text-analysis/

AXA. (2021). *www.axa.es*. https://www.axa.es/sobre-axa-2021

Azure. (2024). *azure.microsoft.com*. https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-azure

Billin. (2023). *billin.net*. https://www.billin.net/glosario/definicion-entidad-aseguradora/

Caicedo Carrillo, J. H. y Rojas Suárez, J. J. (abril de 2018). *Diseño de un sistema de gestión de seguridad de la información para el área de infraestructura tecnológica de Alfragres S.A*

: basado en la norma ISO / IEC 27001:2013. https://repository.unipiloto.edu.co/handle/20.500.12277/2714

CampusCiberseguridad. (2023). *campusciberseguridad.com*. https://www.campusciberseguridad.com/blog/item/118-tipos-de-vulnerabilidades-en-ciberseguridad

Chubb. (2024). *https://about.chubb.com*. https://about.chubb.com/

CISCO. (2024). *cisco.com*. https://www-cisco-com.translate.goog/c/en_au/products/security/firewalls/what-is-a-next-generation-firewall.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc#~choose-an-ngfw-firewall

cisecurity. (2024). *cisecurity.org*. https://www-cisecurity-org.translate.goog/controls?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

clientify. (2024). *clientify.com*. https://clientify.com/blog/marketing/recoleccion-de-datos-metodos-tecnicas-e-instrumentos

Cloudfare. (2023). *cloudfare.com*. https://www.cloudflare.com/es-es/learning/security/threats/owasp-top-10/

concepto. (5 de agosto de 2021). *www.concepto.de*. https://concepto.de/metodos-de-investigacion/

Dávila Angeles, A. y Dextre Alarcón, B. (2021). *repositorio.utp.edu*.://hdl.handle.net/20.500.12867/4906

Deflino, D. (2024). *delfino.cr*. https://delfino.cr/2024/12/siete-ciberataques-que-impactaron-america-latina-en-2024

EASYDMARC. (2023). *easydmarc.com*. https://easydmarc.com/blog/es/las-8-causas-mas-comunes-de-una-violacion-de-datos/

Economipedia. (2021). *economipedia.com*. https://economipedia.com/definiciones/investigacion-mixta.html

eset. (2024). *www.eset.com*. https://www.eset.com/py/acerca-de-eset/sala-de-prensa/comunicados-de-prensa/articulos-de-prensa/vulnerabilidades-mas-destacadas-en-2024/

fastercapital. (2022). *fastercapital.com*. https://fastercapital.com/es/palabra-clave/observaci%C3%B3n-estructurada.html

Fortra. (2024). *fortra.com*. https://www.fortra.com/es/recursos/guias/automatizacion-de-procesos-5-principales-beneficios-en-empresas

google. (07 de enero de 2025). *cloud.google.com*. https://cloud.google.com/dialogflow/cx/docs/concept/conversation-history?hl=es-419

guru99. (2023). *guru99.com*. https://www.guru99.com/es/vulnerability-scanning-tools.html

Hernández-Sampieri, R. (2018). *Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta.* Mc Graw Hill.

IAIS. (setiembre de 2019). *iais.com*. https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://a2ii.org/en/media/3338/download&ved=2ahUKEwi51-rSrt-KAxXERjABHZIjBhIQFnoECCMQAQ&usg=AOvVaw2ye4Pb_9Lgr8uHCAOD_wI7

IBM. (2022). https://www.ibm.com/es-es/topics/infraestructure

IBM. (2022). https://www.ibm.com/es-es/topics/intrusion-detection-system

IBM. (24 de agosto de 2022). https://www.ibm.com/docs/es/integration-bus/10.0?topic=service-chef

ibm. (2022). *ibm.com*. https://www.ibm.com/mx-es/topics/automation

IBM. (2023). https://www.ibm.com/es-es/topics/data-exfiltration

IBM. (diciembre de 2023). https://www.ibm.com/es-es/topics/vulnerability-scanning

IBM. (2023). https://www.ibm.com/es-es/topics/zero-day

IBM. (2023). https://www.ibm.com/es-es/topics/cyber-risk-management

IBM. (2024). https://www.ibm.com/es-es/topics/intrusion-detection-system

IBM. (2024). https://www.ibm.com/es-es/topics/incident-management

IBM. (mayo de 2024). https://www.ibm.com/think/topics/phishing

IBM. (2024). https://www.ibm.com/mx-es/think/topics/man-in-the-middle

INA. (2023). *www.ina.ac.cr*. https://www.ina-pidte.ac.cr/pluginfile.php/15090/mod_resource/content/10/idm-2/pdf/pdf-formulas.pdf

INCIBE. (2024). https://www.incibe.es/ciudadania/blog/que-son-los-ataques-dos-y-ddos

INCIBE. (2024). https://www.incibe.es/aprendeciberseguridad/vulnerabilidad

incibe. (2024). *incibe.es*. https://www.incibe.es/empresas/blog/sistemas-edr-son-y-ayudan-proteger-seguridad-tu-empresa

INS. (2024). *grupoins.com*. https://www.grupoins.com/nosotros/somos-grupo-ins/

INS, D. d. (2022). Organigrama Dirección de TI. *Organigrama Dirección de TI*.

InvestigaliaCR. (2023). *investigaliacr.com*. https://investigaliacr.com/investigacion/el-enfoque-de-investigacion-la-naturaleza-del-estudio/

ISO. (10 de 2022). https://www.iso.org/es/contents/data/standard/08/28/82875.html

ISO. (2022). *iso.org*. https://www.iso.org/standard/27001

Jaen, U. (2023). *web.ujaen.es*. https://web.ujaen.es/investiga/tics_tfg/pdf/cualitativa/recogida_datos/recogida_observacion.pdf

Jaramillo Castillo, C. M. y Riofrío Herrera, J. C. (febrero de 2015). *Metodología para realizar la evaluación, detección de riesgos, vulnerabilidades y contramedidas en el diseño e implementación de la infraestructura de la red de la Editorial Don Bosco, mediante un test de intrusión de caja blanca*. https://dspace.ups.edu.ec/handle/123456789/7910

Karpersky. (2024). *karpersky.es*. https://www.kaspersky.es/resource-center/definitions/brute-force-attack

Karspersky. (2024). https://www.kaspersky.es/resource-center/definitions/what-is-a-cross-site-scripting-attack

Karspersky. (2024). *latam.karspersky.com*. https://latam.kaspersky.com/about/press-releases/america-latina-enfrenta-mas-de-31-millones-de-ataques-de-malware-por-dia-alerta-kaspersky?srsltid=AfmBOoqprNT_GxjtLkc7GdrQfZ2ivs4DvKXZla55sDTdzRfOmgicOBlR

KPMG. (2024). *kpmg.com*. https://www.tendencias.kpmg.es/2020/12/ciberseguridad-sector-seguros-afrontar-riesgos-nueva-regulacion/

Leiva Montero, A. C., Mantilla Quesada, L. A. y Córdoba Retana, J. (2022). *Propuesta de un modelo de ciberseguridad para la pequeña empresa en Costa Rica*. https://repositorio.ulacit.ac.cr/bitstream/handle/20.500.14230/10860/REF-1661624621-2.pdf?sequence=2&isAllowed=y

maestriasydiplomadostec. (21 de marzo de 2023). *www.maestriasydiplomados.tec.mx*. https://blog.maestriasydiplomados.tec.mx/recoleccion-de-datos-que-es-ventajas-y-consejos-para-usarlos

Mejía Escobar, A. (2020). *repository.unad.edu.co*. https://repository.unad.edu.co/bitstream/handle/10596/34626/amejiaes.pdf

MetLife. (2024). *www.metlife.com*. https://www.metlife.com/about-us/corporate-profile/

MICITT. (2023). *Estrategia nacional de ciberseguridad de costa rica 2023-2027*. https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf

MICROSOFT. (2024). *microsoft.com*. https://www.microsoft.com/es-es/security/business/security-101/what-is-siem

Microsoft. (2024). *www.microsoft.com*. https://www.microsoft.com/es-es/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024

Mundial, F. E. (2024). *weforum*. https://es.weforum.org/stories/2024/10/foco-en-la-ciberseguridad-10-cosas-que-necesitas-saber-en-2024/

NIST. (2024). *nist-gov*. https://www-nist-gov.translate.goog/itl/smallbusinesscyber/nist-cybersecurity-framework-0?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

OpenWebinars. (2024). *openwebinars.net*. https://openwebinars.net/blog/escaneo-de-vulnerabilidades/

OWASP. (2024). *owasp.org*. https://owasp-org.translate.goog/www-community/attacks/Command_Injection?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

paloaltonetworks. (2024). *paloaltonetworks*. https://www-paloaltonetworks-ca.translate.goog/cyberpedia/what-is-soar?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Paloaltonetworks. (2024). *paloaltonetworks.com*. https://www-paloaltonetworks-com.translate.goog/cyberpedia/what-is-extended-detection-response-XDR?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

PALOALTONETWORKS. (2024). *paloaltonetworks-com.*: https://www-paloaltonetworks-com.translate.goog/cyberpedia/what-is-an-intrusion-prevention-system-ips?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

paloaltonetworks-com. (2024). https://www-paloaltonetworks-com.translate.goog/cyberpedia/what-is-an-intrusion-prevention-system-ips?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Pazmiño López, L. A. (2017). *Diseño de una metodología para la detección de ataques a infraestructuras informáticas basada en la correlación de eventos*. http://dspace.espoch.edu.ec/handle/123456789/7817

Porto, J. P. (2008). *Definicion.de*. https://definicion.de/empresa/

Pérez Porto, J. (2017). *definicion.de*. https://definicion.de/empresa/

Quesada Artavia, D. (mayo de 2022). *Ciberataques y su análisis desde la óptica penal*. https://ministeriopublico.poder-judicial.go.cr/index.php/medios-informativos/noticias-judiciales/ciberataques-y-su-analisis-desde-la-optica-penal

QuestionPro. (29 de agosto de 2022). *www.questionpro.com*. www.questionpro.com: https://www.questionpro.com/blog/es/que-es-una-poblacion/

recursos.ucol. (2024). *recursos.ucol.mx*. https://recursos.ucol.mx/tesis/investigacion.php

Redhat. (2018). *redhat.com*. https://www.redhat.com/es/topics/security/what-is-malware?gad_source=1&gclid=CjwKCAiAmrS7BhBJEiwAei59i7kkpbosW9902ApVLQYY_TyW2BrkkxplavyXcNY78DxLFV_2WeQPMBoCCjoQAvD_BwE

RedHat. (21 de junio de 2022). https://www.redhat.com/es/topics/automation/learning-ansible-tutorial?gad_source=1&gclid=Cj0KCQiAj9m7BhD1ARIsANsIIvAgmfwT94cDA6qZ0LUo8N66uB23nNXSUssLm0HE6YBiIQGNIno77zQaAjysEALw_wcB

RedHat. (2024). *redhat.com*. https://www.redhat.com/es/topics/security/what-is-soar?gad_source=1&gclid=Cj0KCQiAyc67BhDSARIsAM95QzuCuPdJNSY-GfdjNkTL94MSdYgWWqc648neBI40TNM5_BQGYA63OZ0aAmdMEALw_wcB

Reyes Narvaez, J. (22 de 11 de 2011). *Servicio de detección temprana de vulnerabilidades basado en Shodan: caso de estudio ESPE-CERT*. https://repositoriobe.espe.edu.ec/server/api/core/bitstreams/39c60e75-de43-41f2-9449-0de97e08fd63/content

safecore. (2023). *safecore.io*. https://safecore.io/es/industries/la-cyber-security-nel-settore-assicurativo-lo-scenario-i-rischi-e-le-sfide-future/

SAP. (2022). *sap.com*. https://www.sap.com/latinamerica/products/technology-platform/process-automation/what-is-process-automation.html

Solarte Castañeda, C. (setiembre de 2021). *Evaluación de la Existencia de Políticas de Ciberseguridad en las Pymes y en las organizaciones del sector público que no tienen personal de ciberseguridad en Costa Rica*. https://repositorio.ucenfotec.ac.cr/bitstream/handle/123456789/379/Solarte%20Casta%C3%B1eda%20C%C3%A9sar-MSEG_oct2021.pdf?sequence=1&isAllowed=y

Splunk. (2024). *splunk.com*. https://www-splunk-com.translate.goog/en_us/blog/learn/what-splunk-does.html?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Tenable. (2023). *www.tenable.com*. https://es-la.tenable.com/products/nessus

TheBridge. (2023). *thebridge.tech*. https://thebridge.tech/blog/que-es-un-red-team

Toala Arias, F. y Mazamba Muñoz, J. (Noviembre de 2023). *repositorio,unesum.edu.ec*. http://repositorio.unesum.edu.ec/handle/53000/5930

UGR.ES. (2021). *www.ugr.es*. https://www.ugr.es/~anamaria/fuentesws/Intro-FI.htm

UNIR. (2024). *www.unir.net*. https://www.unir.net/revista/marketing-comunicacion/monitorizar-redes-sociales/

Valencia, U. d. (2022). *www.uv.es*. https://www.uv.es/cibisoc/tutoriales/trabajo_social/22_las_fuentes_de_informacin.html

Villafuerte Guerrero, M. (2021). *Estrategia para la gestión de políticas de seguridad informática en una municipalidad de la Región Chorotega*. https://www.kerwa.ucr.ac.cr/server/api/core/bitstreams/740c4b7f-0dc6-4dd4-b727-1f087fd73e89/content

VIU, U. (2022). *www.universidadviu.com*. https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-observacion-no-participante-y-que-usos-tiene

APÉNDICES

Entrevista #1:

Principio del formulario

Entrevista 1

Entrevista para el director de TI del INS

¿Cuál es su rol principal en la gestión de la infraestructura tecnológica del INS?

Tu respuesta

¿Cómo se involucra su equipo en la detección y corrección de vulnerabilidades?

Tu respuesta

¿Qué herramientas utilizan actualmente para la detección de vulnerabilidades?

Tu respuesta

¿Cuál es el tiempo promedio que toma identificar y corregir una vulnerabilidad crítica?

Tu respuesta

¿Cuáles son las principales limitaciones del proceso manual en términos de eficiencia y precisión?

Tu respuesta

En su opinión, ¿cómo podría la automatización mejorar los tiempos de respuesta ante vulnerabilidades?

Tu respuesta

¿Qué aspectos técnicos considera más desafiantes en la implementación de un sistema automatizado?

Tu respuesta

¿Cómo afectará la automatización a la carga de trabajo de su equipo?

Tu respuesta

¿La infraestructura actual del INS está preparada para integrar un sistema automatizado?

Tu respuesta

¿Qué integraciones considera esenciales entre el sistema automatizado y las herramientas actuales de monitoreo o gestión?

Tu respuesta

¿Qué riesgos o desafíos de seguridad percibe al automatizar este proceso?

Tu respuesta

¿Cómo garantizar que el sistema automatizado sea confiable y se mantenga actualizado frente a nuevas vulnerabilidades?

Tu respuesta

¿El personal de TI tiene el conocimiento técnico necesario para gestionar una herramienta automatizada?

Tu respuesta

¿Qué tipo de capacitación o recursos considera necesarios para una implementación exitosa?

Tu respuesta

¿Qué beneficios estratégicos cree que podría aportar la automatización al INS en términos de seguridad y eficiencia?

Tu respuesta

¿Qué recomendaciones daría para asegurar una transición exitosa hacia la automatización?

Tu respuesta

Entrevista #2:

Entrevista 2

Entrevista para el encargado de Seguridad de TI en la Organización

¿Cuál es su visión general sobre el estado actual de la seguridad tecnológica del INS?

Tu respuesta

¿Cómo se alinean las políticas de seguridad actuales con los procesos de detección y corrección de vulnerabilidades?

Tu respuesta

Desde su perspectiva, ¿qué tan efectivo es el proceso actual para gestionar vulnerabilidades críticas?

Tu respuesta

¿Qué brechas en la seguridad identifica en el proceso manual actual?

Tu respuesta

¿Cómo cree que la automatización del proceso contribuirá a mitigar riesgos de seguridad?

Tu respuesta

¿Qué impacto tendrá la automatización en el cumplimiento de normativas como ISO 27001 o el marco NIST?

Tu respuesta

¿Qué controles considera esenciales para asegurar la efectividad del sistema automatizado?

Tu respuesta

¿Cómo planea medir y gestionar los riesgos asociados a la implementación de la automatización?

Tu respuesta

¿Qué tan preparada está la organización para adoptar cambios relacionados con la automatización?

Tu respuesta

¿Qué medidas sugiere para promover una cultura de seguridad que respalde el uso de herramientas automatizadas?

Tu respuesta

¿Qué métricas utilizará para evaluar el éxito de la automatización en términos de seguridad?

Tu respuesta

¿Qué desafíos estratégicos anticipa durante y después de la implementación?

Tu respuesta

Desde su perspectiva como Encargado de Seguridad de TI, ¿qué factores son clave para una implementación exitosa?

Tu respuesta

¿Qué consejos le daría al equipo técnico y a la alta gerencia para garantizar el éxito del proyecto?

Tu respuesta

Encuesta:

Encuesta 1

Automatización del proceso de detección y corrección de vulnerabilidades

¿Cuál es su rol dentro de la organización?

Administrador de sistemas

Ingeniero en Seguridad

Analista de TI

Otro (especifique):

¿Cuántos años de experiencia tiene en el área de TI?

Menos de 1 año

1-3 años

4-6 años

Más de 6 años

En una escala del 1 al 5, evalúe su conocimiento sobre las vulnerabilidades más comunes en la infraestructura tecnológica

Muy bajo

Bajo

Moderado

Alto

Muy alto

¿Con qué frecuencia detecta vulnerabilidades críticas en la Infraestructura del INS?

Nunca

Rara vez

A veces

Frecuentemente

Siempre

En una escala del 1 al 5 ¿cómo evaluaría la eficiencia del proceso actual de detección de vulnerabilidades?

Muy ineficiente

Ineficiente

Neutral

Eficiente

Muy Eficiente

¿Qué tan satisfecho está con la herramienta actual utilizada para la detección de vulnerabilidades?

Muy insatisfecho

Insatisfecho

Neutral

Satisfecho

Muy satisfecho

¿El tiempo promedio de corrección de vulnerabilidades críticas es adecuado?

Totalmente en desacuerdo

En desacuerdo

Neutral

De acuerdo

Totalmente de acuerdo

¿Qué tan frecuentemente el proceso manual de detección y corrección de vulnerabilidades presenta errores?

Nunca

Rara vez

A veces

Frecuentemente

Siempre

En una escala del 1 al 5, ¿qué tan importante considera la automatización para mejorar la seguridad de la infraestructura tecnológica?

Nada importante

Poco importante

Moderadamente importante

Importante

Muy importante

¿Cree que la automatización reducirá el tiempo promedio de corrección de vulnerabilidades?

Totalmente en desacuerdo

En desacuerdo

Neutral

De acuerdo

Totalmente de acuerdo

¿Qué barreras considera que podrían dificultar la implementación de un sistema automatizado? (Seleccione todas las que apliquen)

Costos

Resistencia al cambio

Falta de conocimiento técnico

Complejidad del sistema actual

Otro:

¿Qué impacto cree que tendría la automatización en la reducción de errores humanos?

Ningún impacto

Poco impacto

Moderado impacto

Alto impacto

Muy alto impacto

En su opinión, ¿cómo afectaría la automatización al cumplimiento de normativas de seguridad (ejemplo: ISO 27001)?

Negativamente

No tendrá impacto

Positivamente

¿Qué tan probable es que la automatización aumente la capacidad de respuesta ante incidentes de seguridad?

Nada probable

Poco probable

Moderadamente probable

Probable

Muy probable

¿El personal actual tiene el conocimiento necesario para manejar sistemas automatizados de detección y corrección?

Totalmente en desacuerdo

En desacuerdo

Neutral

De acuerdo

Totalmente de acuerdo

¿Considera que es necesaria una capacitación específica para implementar un sistema automatizado?

Si

No

¿Cuánto tiempo cree que debería durar una capacitación sobre el nuevo sistema automatizado?

Menos de 1 mes

1-3 meses

4-6 meses

Más de 6 meses

En una escala del 1 al 10, ¿qué tan prioritario considera que es implementar la automatización en el INS?

1: Nada prioritario

10: Muy prioritario

En su opinión, ¿qué funcionalidad es más importante en un sistema automatizado?

Detección en tiempo real

Reportes automáticos

Integración con otras herramientas de seguridad

Otro:

¿Qué recomendaciones daría para la implementación exitosa de un sistema automatizado? (Respuesta abierta)

Tu respuesta

¿Qué tan satisfecho está con la integración actual de herramientas de detección de vulnerabilidades con otras plataformas de seguridad?

Muy insatisfecho

Insatisfecho

Neutral

Satisfecho

Muy satisfecho

¿Qué tan efectiva considera la priorización de vulnerabilidades críticas en el proceso actual?

Totalmente inefectiva

Inefectiva

Neutral

Efectiva

Totalmente efectiva

En su experiencia, ¿con qué frecuencia los equipos de TI logran corregir vulnerabilidades antes de que se conviertan en incidentes?

Nunca

Rara vez

A veces

Frecuentemente

Siempre

¿Cómo describiría el nivel de cooperación entre los equipos responsables de detectar y corregir vulnerabilidades?

Muy deficiente

Deficiente

Neutral

Bueno

Excelente

¿Qué tan útiles son los reportes actuales de vulnerabilidades para la toma de decisiones?

Nada útiles

Poco útiles

Moderadamente útiles

Útiles

Muy útiles

En una escala del 1 al 5, ¿qué tan preparado cree que está el INS para adoptar nuevas tecnologías de automatización en seguridad?

Nada preparado

Poco preparado

Moderadamente preparado

Preparado

Muy preparado

¿Considera que la automatización del proceso permitirá ahorrar recursos económicos en comparación con los métodos manuales?

Totalmente en desacuerdo

En desacuerdo

Neutral

De acuerdo

Totalmente de acuerdo

¿Qué tan confiable cree que será el sistema automatizado para la detección de nuevas vulnerabilidades en comparación con los sistemas manuales?

Nada confiable

Poco confiable

Moderadamente confiable

Confiable

Muy confiable

¿Qué tan probable es que la automatización impulse cambios positivos en la cultura organizacional del INS respecto a la seguridad de TI?

Nada probable

Poco probable

Moderadamente probable

Probable

Muy probable

¿Tiene alguna sugerencia específica para mejorar el proceso de detección y corrección de vulnerabilidades en el INS?

Tu respuesta