REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE
FACULTAD DE POSGRADO
MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A.

Trabajo de Investigación previo a la obtención del Título de Magíster en Computación Con Mención En Seguridad Informática

AUTORA: SAMANTHA MONSERRAT MAFLA FLORES
DIRECTORA: MSC. CRISTINA FERNANDA VACA ORELLANA

IBARRA - ECUADOR

2024

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE
Acreditada Resolución Nro. 173-SE-33-CACES-2020
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	1003637061		
APELLIDOS Y NOMBRES	MAFLA FLORES SAMANTHA MONSERRAT		
DIRECCIÓN	SUCRE 2 29 Y MEJÍA		
EMAIL	smmaflaf@utn.edu.ec		
TELÉFONO FIJO	062952157	**TELÉFONO MÓVIL:**	0967985162

DATOS DE LA OBRA	
TÍTULO:	Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A.
AUTORA:	Mafla Flores Samantha Monserrat
FECHA: DD/MM/AAAA	17/06/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	☐ **PREGRADO** ☒ **POSGRADO**
TITULO POR EL QUE OPTA	Magíster en Computación con Mención en Seguridad Informática
DIRECTORA, ASESOR	**Msc. Cristina Vaca, Msc. Marco Revelo**

CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 17 días del mes de junio del año 2024

AUTORA:

Firma

Nombre: Samantha Monserrat Mafla Flores
CI: 100363706-1

APROBACIÓN DE LA TUTORA

Yo Msc. Cristina Fernanda Vaca Orellana, en calidad de directora de la tesis titulada: **"Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A."** de autoría de la Ing. Samantha Monserrat Mafla Flores, para optar por el grado de Magister en Computación con Mención en Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra a los 17 días del mes de junio del 2024.

Lo certifico

Firmado electrónicamente por:
CRISTINA FERNANDA
VACA ORELLANA

Msc. Cristina Fernanda Vaca Orellana

CI: 1002806535

DIRECTORA DE TESIS

DEDICATORIA

Dedico este proyecto a mi madre, mi mayor fuente de inspiración, quien me ha inculcado valores de integridad y me ha guiado con sabiduría por el sendero correcto. Su ejemplo de perseverancia y dedicación me ha demostrado que con esfuerzo y constancia se pueden alcanzar las metas más anheladas.

A mis sobrinas Lhya y Amelia, cuya presencia llena de luz y alegría mi existencia.

A mi familia, quienes siempre han brindado su incondicional apoyo y aliento, impulsándome a superarme y otorgándome la motivación necesaria para concluir mi carrera con éxito.

Samantha Monserrat Mafla Flores

AGRADECIMIENTO

Expreso mi profunda gratitud hacia mis amados padres, Mónica y Gonzalo, por su inestimable respaldo brindado a través de consejos, comprensión y amor durante los desafíos enfrentados. Agradezco también a mi hermano Damián, mis hermanas Nataly y Ana, y a toda mi familia, cuyo apoyo incondicional y solidaridad fueron un pilar fundamental a lo largo de mi trayectoria académica, impulsándome constantemente a superarme.

Agradezco sinceramente a mi directora, la Msc. Cristina Vaca, y al Msc. Xavier Rosero por su valioso tiempo, paciencia y apoyo incondicional durante todo el proceso de desarrollo de este proyecto.

Con mi profunda gratitud a mi amigo Edison Sánchez, cuyas enseñanzas y respaldo absoluto han sido fundamentales para mi crecimiento profesional. Su guía constante ha sido invaluable en la culminación exitosa de este proyecto.

A mí por nunca rendirme y siempre salir adelante.

Samantha Monserrat Mafla Flores

CONTENIDO

CAPÍTULO I 16

EL PROBLEMA 16

1.1. Planteamiento del problema 16

1.2. Antecedentes 17

1.3. Objetivos de la investigación 19

1.3.1. Objetivo general 19

1.3.2 Objetivos específicos 19

1.4. Justificación 19

CAPÍTULO II 21

MARCO REFERENCIAL 21

2.1. Marco teórico 21

2.1.1. Comunicación asíncrona 21

2.1.2. Seguridad informática y seguridad de la información 22

2.1.3. Controles CIS v.8 22

2.1.4. Norma ISO 27001 ISO/IEC 2022 27002 25

2.1.5. MAGERIT v.3 25

2.1.6. Amenazas y vulnerabilidades informáticas 26

2.2 Herramientas para la gestión de vulnerabilidades 27

2.2.1 Nessus 27

2.2.2 OpenVas 28

2.2.3 Nmap 28

2.3. Marco legal 30

CAPÍTULO III 31

MARCO METODOLÓGICO 31

3.1. Descripción del área de estudio 31

3.2. Enfoque y tipo de investigación 31

3.3. Procedimiento de investigación 32

3.4. Fase 1: Análisis de vulnerabilidades 32

3.4.1 Resultados del análisis de vulnerabilidades 36

3.4.2 Plan de mitigación: Implementación de controles CIS en el servicio de comunicación asíncrona 39

3.5 Fase 2: Implementación de controles CIS v.8 40

3.5.1 Inventario y control de activos empresariales (Control CIS 1) 40

3.5.2 Inventario y Control de activos de software (CIS Control 2): 41

3.5.3 Establecer y mantener un proceso de gestión de datos (Control CIS 3) 41

3.5.4 Configuración segura de activos y software empresariales (Control CIS 4) 42

3.5.5 Administración de cuentas (Control CIS 5) 43

3.5.6 Gestión de control de acceso (Control CIS 6) 43

3.5.7 Gestión continua de vulnerabilidades (Control CIS 7) 44

3.5.8 Protecciones de correo electrónico y navegador web (Control CIS 9) 44

3.6 Fase 3: Implementación metodología MAGERIT v3 45

3.6.1 Determinación de activos 47

3.6.2 Valoración de Activos 49

3.6.3 Identificación de amenazas 51

3.6.4 Valoración de amenazas 52

3.6.5 Estimación de impacto 53

3.6.6 Impacto acumulado 53

3.6.7 Riesgo acumulado e impacto repercutido 55

CAPITULO IV 57

RESULTADOS 57

4.1 Mitigación de vulnerabilidades 57

4.2 Métrica de evaluación 60

4.3 Pentesting 62

CAPITULO V 66

CONCLUSIONES 66

RECOMENDACIONES 67

REFERENCIAS 68

ANEXOS 71

Índice de Tablas

Tabla 1 Objetivos de desarrollo sostenible Fuente: ONU 20

Tabla 2 Riesgos de la comunicación asíncrona Fuente: Autor 21

Tabla 3 Controles CIS básicos Fuente: Autor.....23

Tabla 4 Controles CIS funcionales Fuente: Autor 23

Tabla 5 Controles CIS organizativos Fuente: Autor.....24

Tabla 6 Controles CIS elegidos Fuente: Autor 24

Tabla 7 Pasos de la metodología MAGERIT Fuente: Autor 26

Tabla 8 Clasificación de severidad de vulnerabilidades Fuente: Autor.....27

Tabla 9 Vulnerabilidades encontradas por Nessus 37

Tabla 10 Control CIS 1 Fuente: Autor.....40

Tabla 11 Salvaguardas del Control CIS 2.....41

Tabla 12 Salvaguardas del Control CIS 3.....41

Tabla 13 Salvaguardas del Control CIS 4.....42

Tabla 14 Salvaguardas del Control CIS 5.....43

Tabla 15 Salvaguardas del Control CIS 6.....43

Tabla 16 Salvaguardas del Control CIS 7.....44

Tabla 17 Salvaguardas del Control CIS 9.....44

Tabla 18 Fases de la metodología MAGERIT Fuente: Autor 45

Tabla 19 Dimensiones del método MAGERIT v3 46

Tabla 20 Clasificación de activos. 47

Tabla 21 Activos de la empresa Comercial Hidrobo S.A.....47

Tabla 22 Probabilidad de ocurrencia 52

Tabla 23 Factores de estimación.....53

Tabla 24 Vulnerabilidades SSL 57

Tabla 25 Vulnerabilidad MEMCACHED 57

Tabla 26 Registros de eventos antispam/antivirus por meses.....61

Índice de Figuras

Figura 1 Diagrama del problema de la investigación. Fuente: Autor. 16

Figura 2 Estructura tecnológica de Comercial Hidrobo S.A. Fuente: Autor. 18

Figura 3 Ubicación Comercial Hidrobo – Ibarra. Fuente: Google Maps. 31

Figura 4 Comando de instalación de herramienta Nessus. Fuente: Autor. 32

Figura 5 Comando de inicio y ejecución de Nessus. Fuente: Autor. 33

Figura 6 Dashboard de Nessus. Fuente: Autor. 33

Figura 7 Configuración para escaneo. Fuente: Autor. 33

Figura 8 Opciones de configuración: ajustes generales. Fuente: Autor 34

Figura 9 Opciones de configuración: otros ajustes. Fuente: Autor. 34

Figura 10 Descubrimiento de puertos. Fuente: Autor. 35

Figura 11 Descubrimiento de servicios. Fuente: Autor. 35

Figura 12 Inicio de escaneo. Fuente: Autor. 35

Figura 13 Finalización del escaneo. Fuente: Autor. 36

Figura 14 Resultado del escaneo. Fuente: Autor. 36

Figura 15 Pantalla principal herramienta PILAR. Fuente: Autor. 46

Figura 16 Datos del proyecto. Fuente: Autor. 47

Figura 17 Activos del servicio de comunicación asíncrona. Fuente: Autor. 49

Figura 18 Valoración de activos de servicio de comunicación asíncrona. Fuente: Autor 50

Figura 19 Valoración de dominio del servicio de comunicación asíncrona. Fuente: Autor. 50

Figura 20 Grafica valor/activos. Fuente: Autor. 51

Figura 21 Amenazas del servicio de comunicación asíncrona. Fuente: Autor 51

Figura 22 Amenazas del servicio de comunicación asíncrono. Fuente: Autor 52

Figura 23 Amenazas y probabilidad de ocurrencia. Fuente: Autor 53

Figura 24 Impacto acumulado del servicio de comunicación asíncrona. Fuente: Autor 54

Figura 25 Situación actual del impacto acumulado del servicio de comunicación asíncrona. Fuente: Autor. 54

Figura 26 Riesgo acumulado del servicio de comunicación asíncrona. Fuente:Autor 55

Figura 27 Riesgo acumulado del servicio de comunicación asíncrona Fuente: Autor 56

Figura 28 Riesgo acumulado/dimensión Fuente: Autor 56

Figura 29 Archivo de configuración zmssl.conf Fuente: Autor 58

Figura 30 Archivos de configuración del certificado SSL/TLS 59

Figura 31 Comando de instalación del certificado SSL Fuente: Autor 59

Figura 32 Configuración Memcached. Fuente: Autor 60

Figura 33 Actividad antispam/antivirus. Fuente: Autor 60

Figura 34 Actividad antispam/antivirus después de la aplicación de las salvaguardas. Fuente: Autor 61

Figura 35 Grafica de eventos antispam/antivirus. Fuente: Autor 61

Figura 36 Primer ataque con sploits al servicio de comunicación asíncrona. Fuente: Autor 62

Figura 37 Segundo ataque al servicio de comunicación asíncrona con sploits. Fuente: Autor 63

Figura 38 Dirección IP de la maquina atacante. Fuente: Autor 63

Figura 39 Bloqueo de IP atacante desde el servido. Fuente: Autor 64

Figura 40 Ataque con Metasploit. Fuente: Autor 64

RESUMEN

Este proyecto tiene como objetivo principal la adopción de los controles de seguridad CIS Controls v.8 basados en la Norma ISO/IEC 27001:2022 utilizando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A. La necesidad de mejorar los controles de seguridad en las organizaciones es fundamental para proteger la información confidencial y asegurar la continuidad del negocio. Esta investigación se centra en identificar los controles más adecuados según las mejores prácticas de la norma mencionada y su implementación utilizando la metodología MAGERIT v.3, que permite evaluar y gestionar los riesgos de manera efectiva. Además, se analiza la importancia de mejorar la comunicación asíncrona dentro de las organizaciones, ya que es un aspecto crítico para asegurar la colaboración y la eficiencia en los procesos. Mediante este estudio, se espera proporcionar a las empresas una guía práctica para adoptar los controles de seguridad necesarios y mejorar la comunicación asíncrona en el entorno laboral.

Palabras clave: Controles de seguridad CIS v.8, Metodología MAGERIT, confidencialidad de la información, continuidad de negocio, comunicación asíncrona.

ABSTRACT

This project aims to primarily adopt the CIS Controls v.8 security controls based on ISO/IEC 27001:2022 standard utilizing the MAGERIT v.3 methodology to enhance the asynchronous communication of Comercial Hidrobo S.A. The need to enhance security controls in organizations is essential to safeguard confidential information and ensure business continuity. This research focuses on identifying the most suitable controls according to the best practices of the mentioned standard and their implementation using the MAGERIT v.3 methodology, which enables effective risk assessment and management. Furthermore, it analyzes the importance of improving asynchronous communication within organizations as it is a critical aspect for ensuring collaboration and efficiency in processes. Through this study, it is expected to provide companies with a practical guide to adopting necessary security controls and enhancing asynchronous communication in the workplace.

Keywords: CIS Controls v.8 security controls, MAGERIT methodology, information confidentiality, business continuity, asynchronous communication.

CAPÍTULO I

EL PROBLEMA

1.1. Planteamiento del problema

Comercial Hidrobo S.A. opera un servidor de correo interno alojado físicamente en sus instalaciones, con una dirección IP pública. Este servidor aloja cinco dominios físicos, cada uno con certificados SSL auto firmados. La exposición directa del servidor a Internet se realiza exclusivamente a través del firewall incorporado en el sistema operativo.

La comunicación asíncrona se caracteriza por la transmisión de información sin requerir interacciones en tiempo real entre los participantes. En un entorno empresarial, esto puede incluir el intercambio de correos electrónicos, mensajes instantáneos y documentos compartidos, entre otros medios. Sin embargo, Comercial Hidrobo S.A. no ha implementado las prácticas de seguridad recomendadas para proteger su infraestructura tecnológica y sus datos sensibles, lo que genera vulnerabilidades ante posibles amenazas. Estas vulnerabilidades podrían ser explotadas para llevar a cabo ataques que comprometan la confidencialidad, integridad y disponibilidad de la información.

En el caso específico de esta empresa, se han detectado ataques de phishing dirigidos al servidor de correo, resultando en bloqueos en la recepción y envío de correos electrónicos, así como en la inclusión de los dominios en listas negras a nivel mundial. Las causas subyacentes de estos ataques de phishing se analizan en la Figura 1, presentada como un diagrama de Ishikawa.

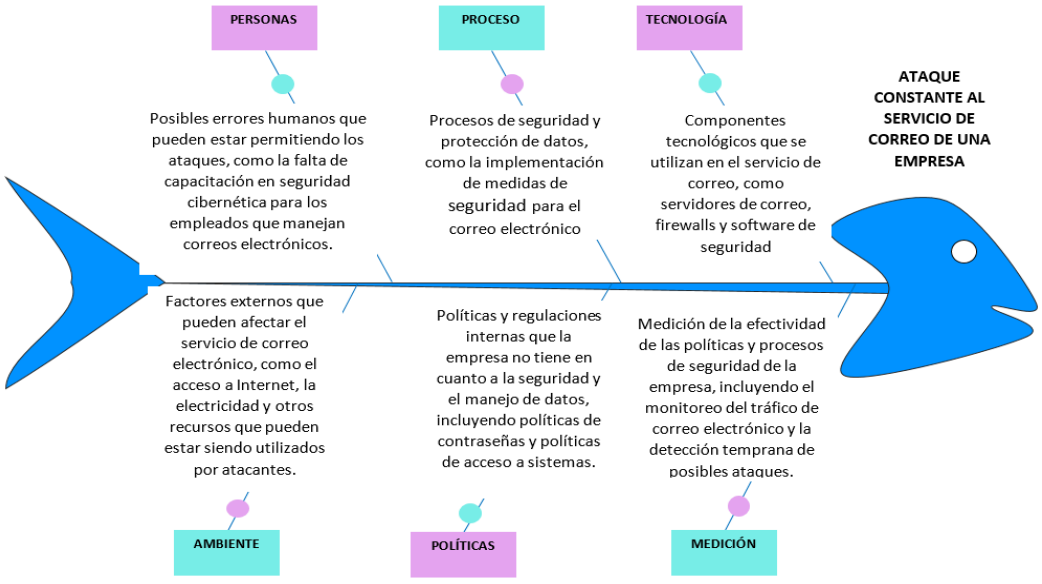


Figura 1 Diagrama del problema de la investigación. Fuente: Autor.

Por consiguiente, se formula la siguiente interrogante como problema de investigación: ¿La adopción de los controles de seguridad CIS v.8 (Center for Internet Security), basados en la Norma ISO/IEC 27001:2022, utilizando la metodología MAGERIT v.3, permite mejorar la comunicación asíncrona en Comercial Hidrobo S.A.?

1.2. Antecedentes

Los ataques cibernéticos tienen como objetivo principal dañar físicamente a las empresas, junto con otros fines como militares o políticos. Entre estos ataques se incluyen el adware, la denegación de servicio distribuido (DDoS), el doxing, los gusanos, el phishing, el ransomware, los troyanos, y los virus, entre otros vectores de ataque (Guaña, 2022). Dos tipos comunes de ataques son el malware, que busca insertar virus, gusanos o troyanos para obtener información del computador infectado, y el phishing, un ataque de ingeniería social diseñado para obtener información confidencial de manera fraudulenta.

Las listas negras contienen direcciones IP identificadas como maliciosas, lo que puede provocar bloqueos en el envío y recepción de correos electrónicos si la IP del servidor de correo se encuentra en alguna de estas listas. Estas listas son de conocimiento público y tienen alcance mundial.

Estas amenazas afectan significativamente a Comercial Hidrobo, ya que permiten a los atacantes obtener acceso al servidor y enviar correos masivos desde los dominios de la empresa, lo que puede llevar a que estos dominios sean incluidos en listas negras y bloqueados para el envío y recepción de correos.

Ejemplos de ataques de phishing conocidos incluyen los enviados en marzo de 2020, durante la pandemia, que se hacían pasar por correos de Microsoft ofreciendo información sobre virus y ataques cibernéticos, pero contenían enlaces de phishing diseñados para robar información. Otro caso conocido fue un ataque de phishing a usuarios de WhatsApp en noviembre de 2019, en el que se enviaban mensajes fraudulentos pidiendo información personal y redirigiendo a un sitio web falso para robar credenciales (González, 2023).

La estructura tecnológica de la empresa incluye múltiples agencias en diferentes ciudades, con una concentración mayor en la ciudad de Ibarra. Todas las oficinas están interconectadas mediante enlaces de fibra óptica y un canal dedicado exclusivamente para la empresa, con enlaces encriptados punto a punto que convergen en la oficina principal, Toyota Ibarra. La administración de los servidores y la salida a internet se realizan desde esta oficina.

La empresa también cuenta con un proveedor de servicios para los enlaces y utiliza un antivirus avanzado como parte del sistema de seguridad del firewall.

El servicio de comunicación asíncrona de la empresa está configurado en un servidor físico de última tecnología, con una vida útil de 5 años. La infraestructura de la empresa se detalla en la Figura 2. Se cuenta con un equipo de respuesta ante incidentes informáticos, conocido como CSIRT, que proporciona información y ayuda para mitigar vulnerabilidades y ataques cibernéticos.

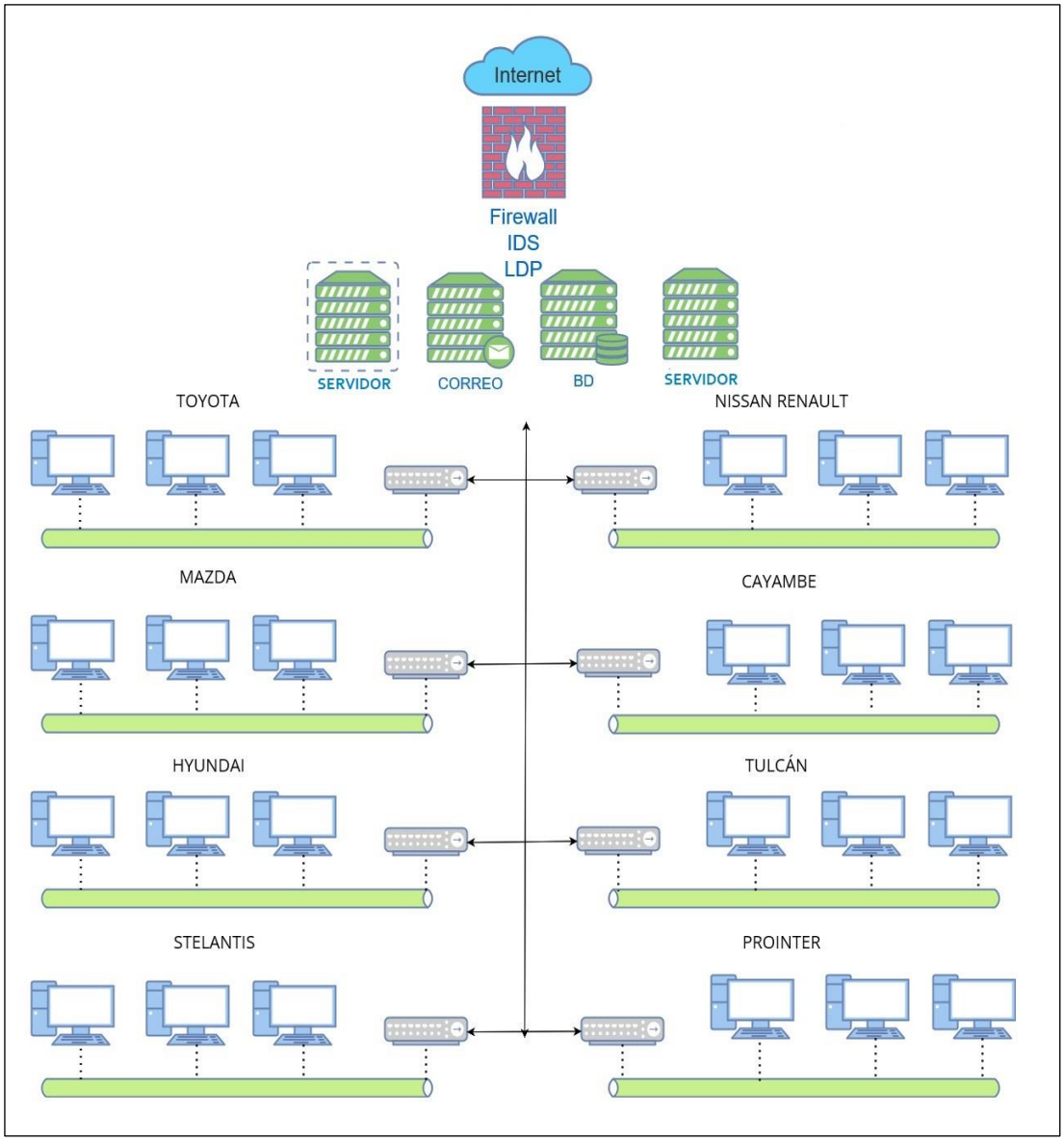


Figura 2 Estructura tecnológica de Comercial Hidrobo S.A. Fuente: Autor.

Investigaciones anteriores han demostrado que la implementación de controles de seguridad mejora la calidad del servicio y mitiga vulnerabilidades en pequeñas y medianas empresas que aún no cuentan con un Sistema de gestión de la Información (SGSI). Por ejemplo,

un estudio realizado en el Instituto Nacional de Evaluación Educativa (INEVAL) resalta la eficacia de estos controles (Honores, 2021).

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Implementar controles de seguridad basados en la Norma ISO/IEC 27001:2022 para el incremento de la eficiencia y seguridad del servicio de comunicación asíncrona de la empresa Comercial Hidrobo S.A.

1.3.2 Objetivos específicos

- Realizar un diagnóstico del servicio de comunicación asíncrona de la Institución mediante escaneos para identificar vulnerabilidades.
- Integrar los controles controles CIS v.8 al servidor de comunicación asíncrona de la Empresa, en conformidad con la Norma ISO/IEC 27001:2022 y la metodología MAGERIT v.3, mitigando las vulnerabilidades identificadas.
- Evaluar el nivel de mejora del servicio de comunicación asíncrona en la Empresa.

1.4. Justificación

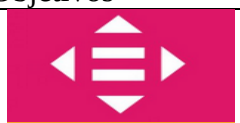
El avance tecnológico se acompaña de crecientes fallas de seguridad que facilitan la vulneración de los sistemas. La explotación de vulnerabilidades de día cero es una táctica común entre los atacantes, quienes aprovechan estos fallos mientras los proveedores de software trabajan en la detección y corrección de los mismos. Mientras tanto, los atacantes buscan obtener la máxima información posible o encriptar los datos de las víctimas que utilicen el software vulnerable (Kaspersky, 2023).

El proyecto se enmarca en la línea de investigación de Desarrollo, Aplicación de Software y Seguridad Cibernética. Esta línea se centra en la elaboración y adaptación de normas de control para proteger la seguridad de los sistemas informáticos y sus datos en línea. En el caso específico del proyecto "Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A.", se prioriza la implementación de los controles CIS. Estos controles son fundamentales para prevenir y

proteger los datos de ciberataques, así como para garantizar la integridad, confidencialidad y disponibilidad de la información.

La adopción de mecanismos de defensa contra la ciberdelincuencia es crucial, especialmente considerando los Objetivos de Desarrollo Sostenible (ODS) mostrados en la Tabla 1, establecidos por la Organización de las Naciones Unidas (ONU). El Objetivo 16 de los ODS es esencial para el desarrollo sostenible, ya que la paz, la justicia y las instituciones sólidas son fundamentales para avanzar en otros ámbitos, como la erradicación de la pobreza, la igualdad de género, la educación de calidad y la protección del medio ambiente (ONU, 2023).

Tabla 1 Objetivos de desarrollo sostenible
Fuente: ONU

Objetivos	Descripción	Objetivos	Descripción
	1 Fin de la pobreza		10 Reducción de las desigualdades
	2 Hambre cero		11 Ciudades y comunidades sostenibles
	3 Salud y bienestar		12 Producción y consumos responsables
	4 Educación de calidad		13 Acción por el clima
	5 Equidad de género		14 Vida submarina
	6 Agua limpia y saneamiento		15 Vida de ecosistemas terrestres
	7 Energía asequible y no contaminante		16 Paz, justicia e instituciones sólidas
	8 Trabajo decente y crecimiento económico		17 Alianzas para lograr los objetivos
	9 industria innovación e infraestructura		

Nota: Adaptado de "Los Objetivos de Desarrollo Sostenible en Ecuador", por Naciones Unidas en Ecuador, 2024, Recuperado de https://ecuador.un.org/es

CAPÍTULO II

MARCO REFERENCIAL

2.1. Marco teórico

2.1.1. Comunicación asíncrona

La comunicación asincrónica, en contraste con la sincrónica, no requiere que los participantes estén presentes en el mismo momento o lugar físico. Se manifiesta en acciones como el envío de correos electrónicos o la participación en foros y wikis. Las respuestas no se obtienen de inmediato, sino después de un periodo de tiempo (Martínez, 2017). A pesar de sus beneficios, como la flexibilidad temporal y la oportunidad de reflexionar antes de responder, la comunicación asíncrona puede presentar desafíos en cuanto a la temporalidad y la claridad de los mensajes. La Tabla 2 detalla algunos de los riesgos asociados con la comunicación asíncrona.

Tabla 2 Riesgos de la comunicación asíncrona
Fuente: Autor

Riesgo	Definición
Intercepción de mensajes	Los mensajes enviados pueden llegar a ser interceptados, dando acceso al atacante al contenido del mensaje e información confidencial.
Suplantación de identidad	El atacante podría hacerse pasar por una persona legítima de alguna entidad, lo que permitiría robar información sensible, logrando el objetivo de suplantar a otra persona.
Malware y phishing	Los mensajes asíncronos pueden contener enlaces maliciosos o documentos que al ejecutarlos o hacerles clic se puede llegar a comprometer la seguridad de su sistema y revelar información confidencial.
Pérdida o robo de dispositivos	La comunicación asíncrona es usada a menudo en dispositivos móviles, por lo que la pérdida de estos dispositivos fácilmente los hace vulnerables.

Errores humanos	Las personas envían información sensible o confidencial por error a algún contacto equivocado. Estos errores pueden resultar en la divulgación inadvertida de información sensible.

2.1.2. Seguridad informática y seguridad de la información

La seguridad informática comprende un conjunto de medidas destinadas a prevenir cualquier actividad no autorizada en sistemas informáticos o de red que pueda ocasionar pérdida o daño de información, comprometiendo su integridad, confidencialidad y disponibilidad, y afectando el rendimiento de los equipos o la conectividad de los usuarios (Gómez, 2014).

Por otro lado, la seguridad de la información va más allá de la seguridad informática, ya que abarca la protección de toda la información de una organización, empresa o entidad pública, garantizando su confidencialidad, integridad y disponibilidad. Esta información puede estar expuesta a diversas amenazas, como el phishing, la propagación de falsas noticias o la inyección de malware (Juan A. Figueroa-Suárez, 2017)

La seguridad de la información implica proteger los datos de una organización, empresa o entidad pública para garantizar su confidencialidad, integridad y disponibilidad. Diversas amenazas, como el phishing, las noticias falsas y la inyección de malware, pueden comprometer la seguridad de la información (Altamirano-de-la-Borda, 2020).

La seguridad de la información se apoya en la seguridad informática para alcanzar su objetivo. Sin embargo, va más allá de esta última, ya que establece pautas para proteger la información en diferentes medios, incluyendo impresos en papel, discos duros y medidas de seguridad relacionadas con el acceso de las personas a dicha información (Juan A. Figueroa-Suárez, 2017).

2.1.3. Controles CIS v.8

Los Controles de seguridad CIS, desarrollados por el Center of Internet Security, son un conjunto de 18 controles diseñados por expertos en ciberseguridad. Estas prácticas se han consolidado como una solución efectiva para prevenir vulnerabilidades y ataques en las empresas (Security, 2021). La maduración de estos controles ha sido posible gracias a una comunidad internacional que comparte información sobre ataques, herramientas y soluciones,

realiza un seguimiento de la evolución de las amenazas y resuelve problemas de forma colaborativa (Honores, 2021).

Los controles CIS v.8 están divididos en tres secciones: controles básicos, controles funcionales y controles organizativos. Esta estructura garantiza que no solo sean una lista de buenas prácticas, sino un conjunto de acciones priorizadas y altamente focalizadas, con el respaldo de una comunidad que los hace implementables, utilizables, escalables y compatibles con todos los requisitos de seguridad.

Los controles básicos se refieren a 6 controles fundamentales que toda empresa debe adoptar para garantizar su disponibilidad y establecer una defensa efectiva contra ataques de ciberseguridad, como se detalla en la Tabla 3.

Tabla 3 Controles CIS básicos
Fuente: Autor

Control	Descripción
Control CIS 1	Inventario y control de activos de hardware
Control CIS 2	Inventario y control de activos de software
Control CIS 3	Protección de datos
Control CIS 4	Configuración segura de activos y software empresarial
Control CIS 5	Gestión de cuentas
Control CIS 6	Gestión de control de accesos

Nota: Adaptado de **"Center for Internet Security"**, por Center for Internet Security, 2024 Recuperado de https://www.cisecurity.org/controls

Los controles funcionales son 10 y están enfocados en la seguridad de la información, con el objetivo de asegurar una protección adecuada frente a amenazas cibernéticas. Cada control se centra en una funcionalidad específica y contribuye a la implementación de una estrategia integral de seguridad, como se muestra en la Tabla 4.

Tabla 4 Controles CIS funcionales
Fuente: Autor

Control	Descripción
Control CIS 7	Gestión continua de vulnerabilidades
Control CIS 8	Gestión de registros de auditoría
Control CIS 9	Protecciones de correo electrónico y navegador web
Control CIS 10	Defensas contra malware
Control CIS 11	Recuperación de datos

Control CIS 12	Gestión de infraestructura de red
Control CIS 13	Monitoreo y Defensa de Redes
Control CIS 14	Concientización sobre seguridad y capacitación en habilidades
Control CIS 15	Gestión de proveedores de servicios
Control CIS 16	Seguridad del software de aplicación

Nota: Adaptado de **"Center for Internet Security"**, por Center for Internet Security, 2024 Recuperado de https://www.cisecurity.org/controls

Los controles organizativos están diseñados para promover una cultura de seguridad sólida en todas las áreas y procesos de la empresa, con el fin de salvaguardar la información. Fomentan una postura proactiva y robusta ante la seguridad, promoviendo prácticas seguras en toda la organización, como se detalla en la Tabla 5.

Tabla 5 Controles CIS organizativos
Fuente: Autor

Control	Descripción
Control CIS 17	Respuesta y gestión de incidentes.
Control CIS 18	Pruebas de penetración.

Nota: Adaptado de **"Center for Internet Security"**, por Center for Internet Security, 2024 Recuperado de https://www.cisecurity.org/controls

De los 18 controles disponibles, la implementación se centra únicamente en aquellos que están directamente relacionados con la comunicación asíncrona, tal como se detalla en la Tabla 6.

Tabla 6 Controles CIS elegidos
Fuente: Autor

Control	Descripción
Control CIS 1	Inventario y control de activos de hardware.
Control CIS 2	Inventario y control de activos de software.
Control CIS 3	Protección de datos.
Control CIS 4	Configuración segura de activos y software empresarial.
Control CIS 5	Gestión de cuentas.
Control CIS 6	Gestión de control de accesos.
Control CIS 7	Gestión continua de vulnerabilidades.
Control CIS 9	Protecciones de correo electrónico y navegador web

Nota: Adaptado de **"Center for Internet Security"**, por Center for Internet Security, 2024 Recuperado de https://www.cisecurity.org/controls

2.1.4. Norma ISO 27001 ISO/IEC 2022 27002

La Norma ISO/IEC 27001 es ampliamente reconocida como el estándar líder a nivel mundial para los sistemas de gestión de seguridad de la información (SGSI). Define los requisitos que deben cumplir estos sistemas y proporciona una guía exhaustiva para la gestión de la seguridad de la información en empresas de todos los tamaños y sectores (ISO, 2022).

Esta norma, creada por expertos en ciberseguridad y emitida por la Organización Internacional de Normalización, ofrece una metodología para la implementación de la seguridad de la información en una empresa. La certificación conforme a la ISO/IEC 27001 implica cumplir plenamente con sus requisitos y es ampliamente adoptada a nivel mundial en el ámbito de la ciberseguridad.

El sistema de gestión de la información (SGSI) al que hace referencia la norma facilita el cumplimiento de los requisitos de la ISO/IEC 27001. Sin embargo, su implementación completa puede resultar costosa y exigir recursos económicos y humanos significativos, lo que puede ser un obstáculo para las medianas y pequeñas empresas. No obstante, es posible abordar la implementación de la norma por secciones, lo que también puede ser una opción viable para asegurar la información de la empresa.

La relación entre la Norma ISO/IEC 27001 y los controles CIS radica en que estos últimos son una herramienta valiosa para cumplir con los requisitos de seguridad de la información establecidos por la norma. Mientras que la norma proporciona una guía general y amplia para la gestión de la seguridad de la información, los controles CIS son más específicos y detallados en su implementación. Al adoptar los controles CIS, la empresa puede enfocarse de manera más efectiva en los riesgos específicos que enfrenta, al tiempo que se alinea con los requisitos generales de la norma.

2.1.5. MAGERIT v.3

MAGERIT v.3, que significa Método de Análisis y Gestión de Riesgos de los Sistemas de Información, responde al proceso de gestión de riesgos, como se detalla en la sección 4.4 dentro del marco de gestión de riesgos. Esta metodología, desarrollada por el Centro Criptológico Nacional de España, proporciona un enfoque estructurado para identificar,

analizar y gestionar los riesgos de seguridad de la información. Consta de 6 pasos, que incluyen la identificación de activos y amenazas, evaluación de riesgos, análisis de vulnerabilidades, diseño de controles de seguridad e implementación, y seguimiento continuo de un plan de seguimiento. Este enfoque ayuda a las organizaciones a proteger sus activos de información y mitigar los riesgos de manera efectiva (España, 2012).

La versión 3 proporciona un marco estructurado para descubrir, analizar y gestionar las amenazas a la seguridad de la información, especialmente en lo que respecta a su aplicación en la comunicación asíncrona. Es crucial considerar las amenazas de seguridad asociadas con la comunicación asíncrona, ya que este tipo de comunicación implica que los participantes no están en contacto directo ni interactúan en tiempo real. Los pasos para utilizar la metodología se detallan en la Tabla 7.

Tabla 7 Pasos de la metodología MAGERIT
Fuente: Autor

N°	Pasos
1	Identificación de activos
2	Análisis de riesgos
3	Valoración de riesgos
4	Tratamiento de riesgos
5	Planificación de la respuesta a incidentes.
6	Seguimiento y revisión

2.1.6. Amenazas y vulnerabilidades informáticas

Se considera una amenaza a cualquier evento accidental o intencionado que pueda causar daños en el sistema informático, lo que resultaría en pérdidas materiales, financieras u otros tipos de perjuicios para la organización (Gómez, 2014). Las amenazas pueden ser de diversos tipos, como naturales (inundaciones, terremotos, etc.), agentes internos (empleados descuidados, mal uso de herramientas tecnológicas) y agentes externos (virus, ataques cibernéticos, etc.). Entre las amenazas más comunes asociadas con la comunicación asíncrona se encuentran el malware, el phishing y el ransomware.

El malware consiste en programas diseñados para insertar virus, gusanos o troyanos en un sistema informático, con el fin de obtener información de manera no autorizada. Por otro lado, el phishing es un tipo de ataque de ingeniería social cuyo objetivo es obtener información

confidencial de manera fraudulenta, mientras que el ransomware es un software que encripta la información, bloqueando el acceso a los datos hasta que se pague un rescate al atacante.

Las vulnerabilidades se refieren a cualquier fallo en el sistema informático que pueda ser explotado por las amenazas para causar daño y pérdidas en la organización (Gómez, 2014). Estos fallos pueden ser de naturaleza lógica o física, como problemas de configuración, ubicación, instalación y mantenimiento. Las causas de las vulnerabilidades incluyen: "debilidades en el diseño de protocolos utilizados en las redes, errores de programación, existencia de puertas traseras, descuido por parte de los fabricantes, configuración inadecuada de los sistemas informáticos y desconocimiento de las herramientas utilizadas en los ataques" (Honores, 2021).

2.2 Herramientas para la gestión de vulnerabilidades

El software desarrollado para el escaneo de vulnerabilidades consiste en programas dedicados a detectar fallos dentro de un sistema operativo o servicio. Estos programas operan en conjunto con bases de datos universales, las cuales se actualizan continuamente con las vulnerabilidades descubiertas día a día.

Este tipo de software se fundamenta en un sistema de puntuación conocido como CVSS (Common Vulnerability Score System), desarrollado por el NIST (National Institute of Standards and Technology). Según el nivel de severidad de las vulnerabilidades detectadas, se clasifican con una puntuación que va del 0 al 10. El NIST define tres niveles de severidad, los cuales se detallan en la Tabla 8.

Tabla 8 Clasificación de severidad de vulnerabilidades
Fuente: Autor

Severidad	Puntaje
Bajo	0.0 – 3.9
Medio	4.0 – 6.9
Alto	2.2 – 10.0

2.2.1 Nessus

Esta herramienta permite: "la detección de activos de alta velocidad, auditoría de configuración, determinación del perfil de objetivo, detección de malware, detección de datos confidenciales" (Tenable, Tenable, 2019). Es una herramienta completa al momento de abordar vulnerabilidades, ya que las detecta y ofrece soluciones para mitigarlas. Además, proporciona

una interfaz gráfica y de consola para su uso adaptable tanto en diferentes sistemas operativos como para diversos usuarios.

Esta herramienta, inicialmente concebida como una plataforma de software libre, en la actualidad se ha transformado en un software privativo, con licencias de pruebas. Ofrece la capacidad de generar reportes personalizados en varios formatos, como XML, HTML, ASCII y LaTex, lo que permite tomar acciones inmediatas y cubrir necesidades específicas en función de cada vulnerabilidad, ya sea por servidor o servicio. Además, cuenta con un entorno web que facilita su control por parte del usuario, guiándolo en el proceso de escaneo. Identifica cada equipo dentro de la red y escanea las posibles vulnerabilidades que podrían existir. Asimismo, notifica las vulnerabilidades y las posibles soluciones a través de correo electrónico. Además, los análisis continúan ejecutándose incluso en caso de desconexión del servidor, y permite el descubrimiento y etiquetado de activos.

2.2.2 OpenVas

Definición tomada de la página oficial: “Es un escáner de vulnerabilidades con todas las funciones. Sus capacidades incluyen pruebas autenticadas y no autenticadas, varios protocolos industriales y de Internet de alto y bajo nivel, y ajuste de rendimiento para escaneos a gran escala” (OpenVas, 2023). Cuenta con una interfaz de comandos OpenVas CLI o una plataforma web Greenbone Security Assistant para su uso. Proporciona reportes claros y completos, la capacidad de realizar escaneos a varios equipos simultáneamente, y un gestor que filtra y clasifica los resultados de los análisis. Además, su uso en Linux es menos complejo que en otros sistemas operativos, aunque el tiempo de análisis es prolongado en comparación con otros softwares.

2.2.3 Nmap

Sus siglas significan mapeador de redes, es una herramienta de exploración de red y auditoría de seguridad de software libre. Mayormente utilizada para auditorías de seguridad, Nmap emplea paquetes IP "crudos" en sus formas originales para determinar la disponibilidad de equipos en una red, los servicios que ofrecen (incluyendo nombre y versión de la aplicación), los sistemas operativos que ejecutan (junto con sus versiones), el tipo de filtros de paquetes o cortafuegos que se están utilizando, entre otras características (Fyodor, 2023).

Entre sus características se destacan la identificación de equipos en la red, su portabilidad, facilidad de uso y flexibilidad. Además, Nmap permite la detección de

vulnerabilidades y el escaneo de puertos y redes. Su naturaleza de software libre posibilita la personalización tanto en la configuración como en el comportamiento de la herramienta. Además, cuenta con una variedad de paquetes o plugins adicionales para explotar otros tipos de vulnerabilidades. En la Tabla 9 se identifican y comparan las características principales de las tres herramientas analizadas anteriormente.:

Tabla 9 Comparación de herramientas para la gestión de vulnerabilidades
Fuente: Autor

Característica	Nessus	OpenVas	Nmap
Libre	Sí	Sí	Sí
Identificación de equipos	Sí	Sí	Sí
Clasificación de vulnerabilidades	Sí	Sí	Sí
Solución a vulnerabilidades	Sí	No	No
Multiplataforma	Sí	Sí	Sí
Análisis de tráfico en tiempo real	Sí	No	No
Generación de reportes	Sí	Sí	Sí

Una vez examinadas las características principales y más relevantes de las tres herramientas seleccionadas para el escaneo de vulnerabilidades, se determina lo siguiente. OpenVas, al ser software libre, no requiere licencia y ofrece capacidades de detección y sugerencias de solución de vulnerabilidades. Sin embargo, su limitación radica en la base de datos a la cual está ligada, que no es muy extensa. Nmap se centra principalmente en las vulnerabilidades de una red, mostrando excelencia en esta área. No obstante, sus reportes están limitados a un formato XML, lo que podría mejorarse para incluir funcionalidades como la generación de mapas de red.

La herramienta elegida es Nessus, reconocida por ser completa y una de las más utilizadas actualmente para la detección de vulnerabilidades. Su versión gratuita incluye todas las opciones y paquetes necesarios para el escaneo requerido. Los reportes que genera permiten una mejor identificación de las vulnerabilidades y proporcionan pautas para su mitigación. Además, utiliza diversas bases de datos de vulnerabilidades, lo que aumenta la detección y las

soluciones ofrecidas. Por último, se ajusta a las plantillas de configuración de los controles CIS que se implementarán en la empresa.

2.3. Marco legal

El presente tema de investigación se rige por las leyes establecidas en la Constitución ecuatoriana, así como por la Ley de Protección de Datos Personales, que incluye los artículos: Artículo 7 "Tratamiento legítimo de los datos", Artículo 8 "Consentimiento", Artículo 12 "Derecho a la información" y Artículo 13 "Derecho de acceso" (Ecuador, 2021). La empresa en la que se desarrolla la investigación cuenta con una "Política de Sistemas Informáticos" que sirve de guía para el desarrollo del proyecto (Sánchez, Intranet, 2020).

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio

El proyecto presentado se lleva a cabo en la ciudad de Ibarra, específicamente en la empresa Comercial Hidrobo S.A., como se muestra en la Figura 3. Esta empresa se dedica a ofrecer servicios automotrices, incluyendo la venta de vehículos nuevos y usados, así como servicios de posventa, como repuestos y taller mecánico. Está ubicada en la Av. Mariano Acosta y Lucio Tarquino Páez.

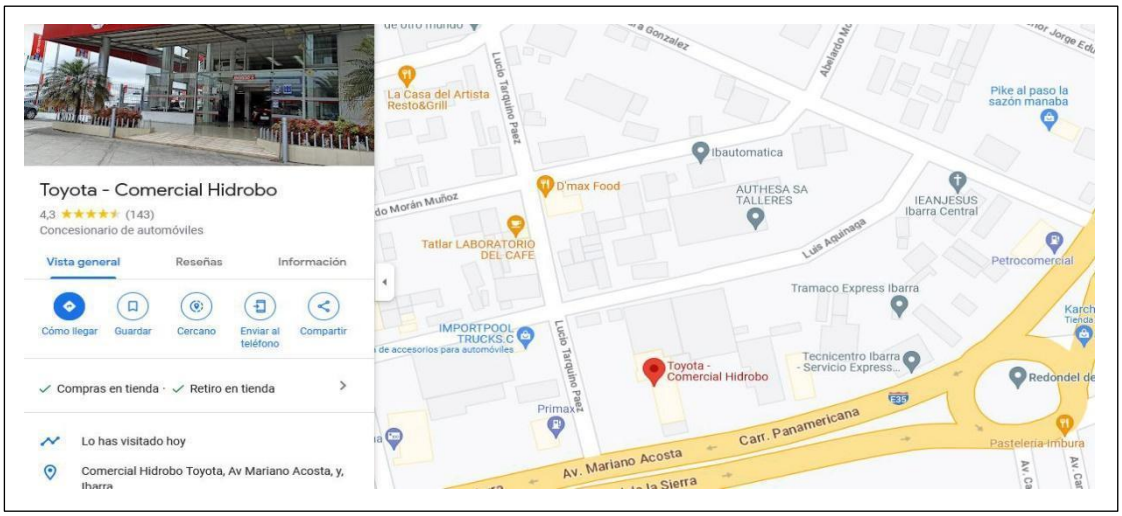


Figura 3 Ubicación Comercial Hidrobo – Ibarra. Fuente: Google Maps.

En cuanto a la población para la investigación, se consideran todos los colaboradores de Comercial Hidrobo, que son 100 personas. Esta misma población se toma como muestra para la realización del trabajo. Para dicha muestra se dispone de un acuerdo de confidencialidad que se visualiza en el **ANEXO 1**.

3.2. Enfoque y tipo de investigación

El enfoque adoptado para abordar el problema de investigación es cuantitativo, con el objetivo de determinar el porcentaje de mejora en la comunicación asíncrona después de la aplicación de los controles CIS para prevenir futuros ciberataques. Para medir esta mejora, se propone realizar un análisis de vulnerabilidades antes y después de la implementación de los controles, con el fin de comparar los resultados y determinar el nivel de optimización de la seguridad en la comunicación asíncrona. Esta investigación se enmarca dentro de un enfoque descriptivo y de campo. Se lleva a cabo un análisis de las medidas cibernéticas implementadas

en la empresa, así como de los controles CIS v.8 aplicables a la misma, con el propósito de mejorar el servicio de comunicación asíncrona. Además, se invita a los usuarios finales a participar en el estudio, con el objetivo de recopilar información sobre su experiencia y percepción acerca de la eficacia de las medidas implementadas para prevenir ataques cibernéticos.

3.3. Procedimiento de investigación

Se inicia con un análisis de vulnerabilidades para evaluar el estado actual del servicio de comunicación asíncrona, con el objetivo de identificar los puntos vulnerables que requieren atención en la investigación subsiguiente. Una vez completado el análisis, se emplea la Metodología MAGERIT v.3 para determinar los problemas más relevantes. A continuación, se seleccionan los controles CIS para que sean adaptables a la empresa. Finalmente, se lleva a cabo una comparación entre la situación previa y posterior a la implementación de los controles CIS, evaluando cómo estos han optimizado la comunicación asincrónica.

3.4. Fase 1: Análisis de vulnerabilidades

Se lleva a cabo un proceso crucial para identificar posibles debilidades en el servicio de comunicación asíncrona. Este análisis abarca la evaluación minuciosa de los diferentes componentes del servicio, como servidores, clientes, protocolos de comunicación y sistemas de autenticación. El objetivo primordial es asegurar la integridad, confidencialidad y disponibilidad de la comunicación asíncrona, mediante la detección y análisis exhaustivo de las vulnerabilidades presentes. Para este propósito, se emplea la herramienta Nessus en su versión Essentials, la cual permite realizar el escaneo de vulnerabilidades y generar informes de forma gratuita.

La instalación de Nessus se inicia con la ejecución de los comandos correspondientes (Figura 4), seguida por el inicio de sesión en la plataforma. Una vez completada la instalación, se accede al dashboard de Nessus (Figuras 5 y 6) y se procede con la configuración para el escaneo (Figuras 7, 8 y 9).

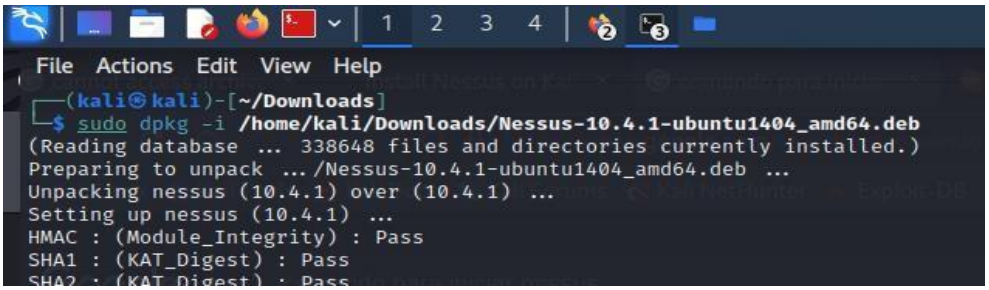


Figura 4 Comando de instalación de herramienta Nessus. Fuente: Autor.

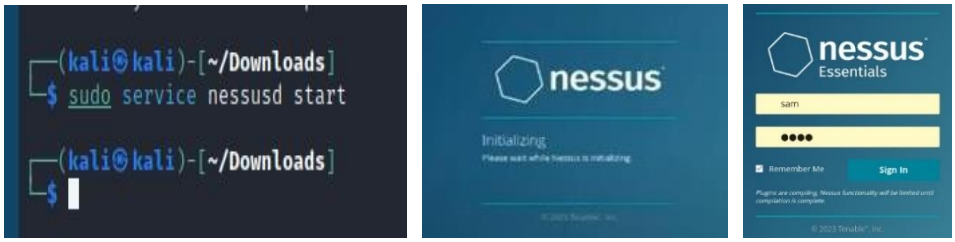


Figura 5 Comando de inicio y ejecución de Nessus. Fuente: Autor.

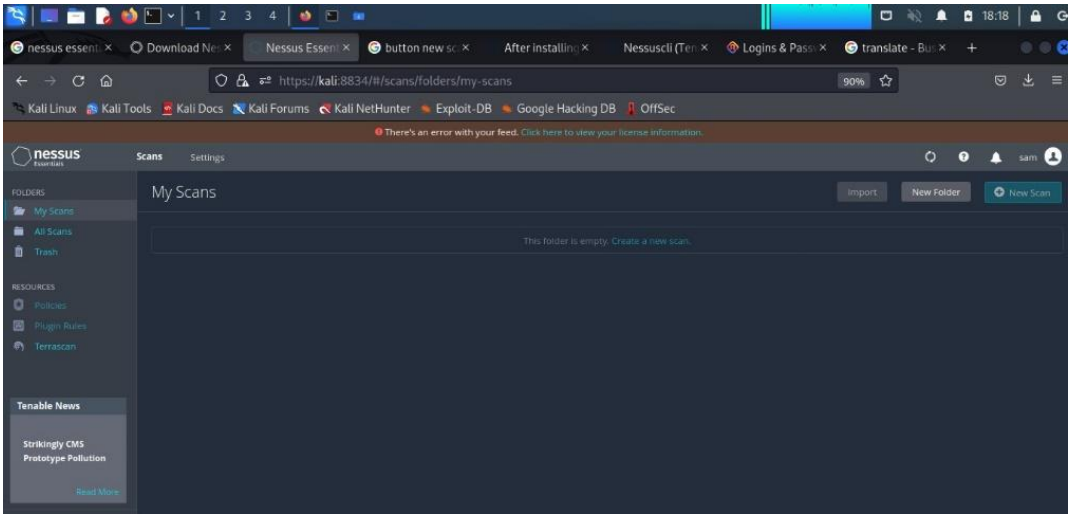


Figura 6 Dashboard de Nessus. Fuente: Autor.

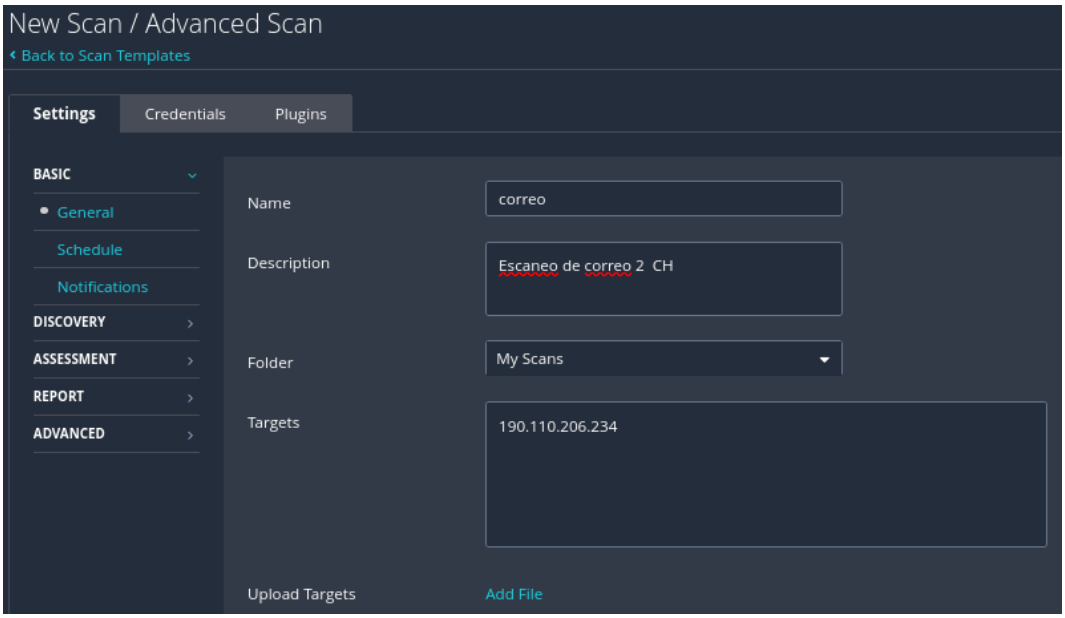


Figura 7 Configuración para escaneo. Fuente: Autor.

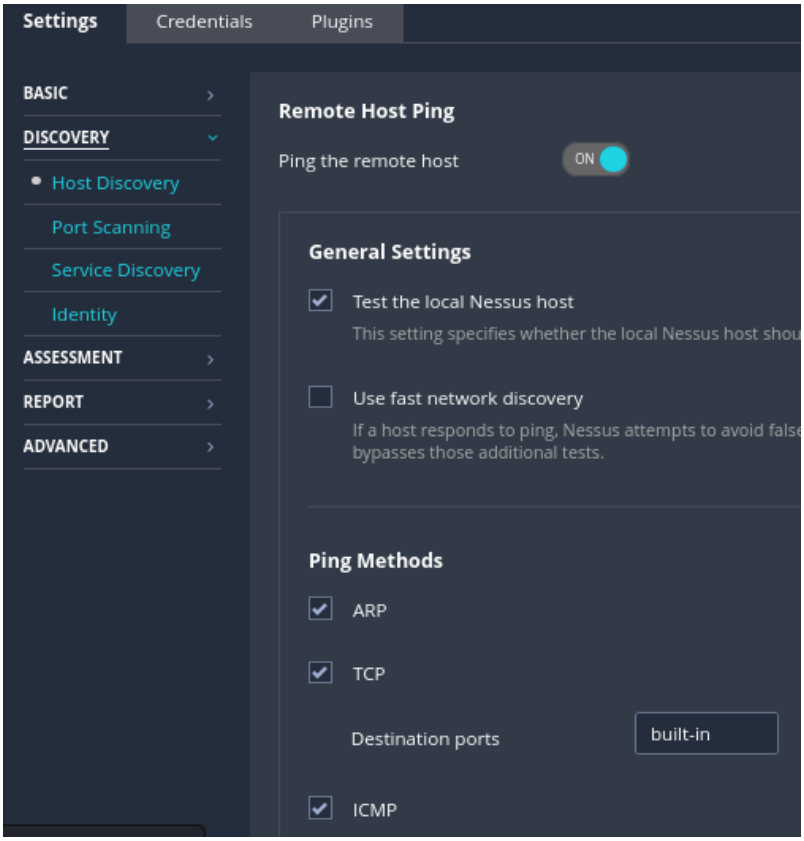


Figura 8 Opciones de configuración: ajustes generales. Fuente: Autor.

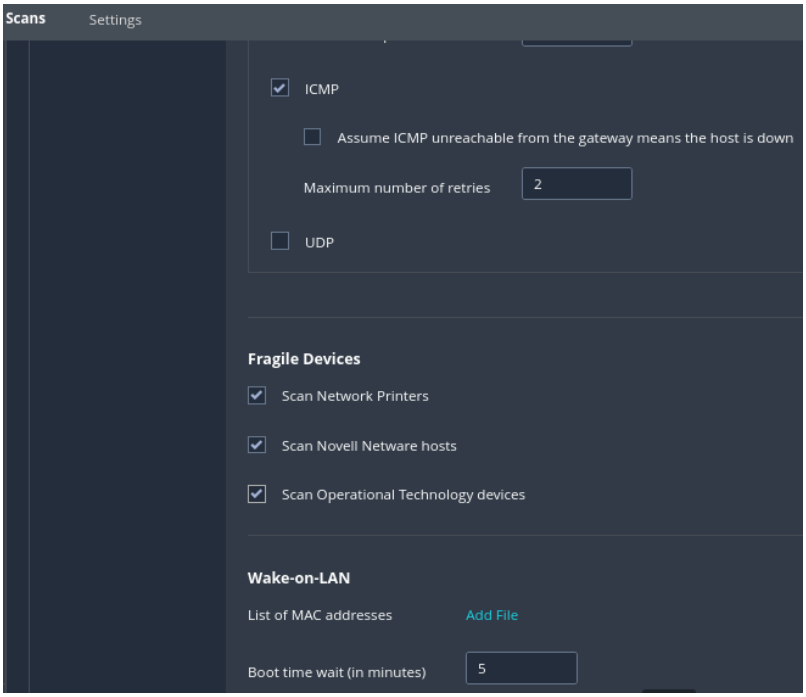


Figura 9 Opciones de configuración: otros ajustes. Fuente: Autor.

La configuración implica establecer las opciones de descubrimiento de host, Figura 10, y los puertos y servicios, Figura 11, seleccionando las configuraciones adecuadas para un escaneo completo y detallado.

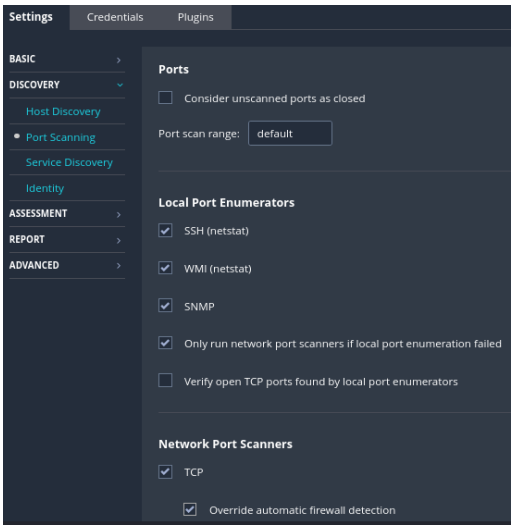


Figura 10 Descubrimiento de puertos. Fuente: Autor.

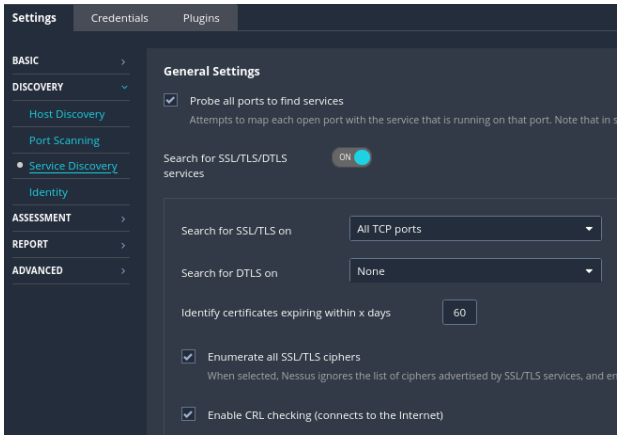


Figura 11 Descubrimiento de servicios. Fuente: Autor.

Una vez iniciado el escaneo se observa el avance del mismo, como se indica en la Figura 12.

Figura 12 Inicio de escaneo. Fuente: Autor.

Al cabo de varios minutos el resultado del escaneo se presenta en la Figura 13.

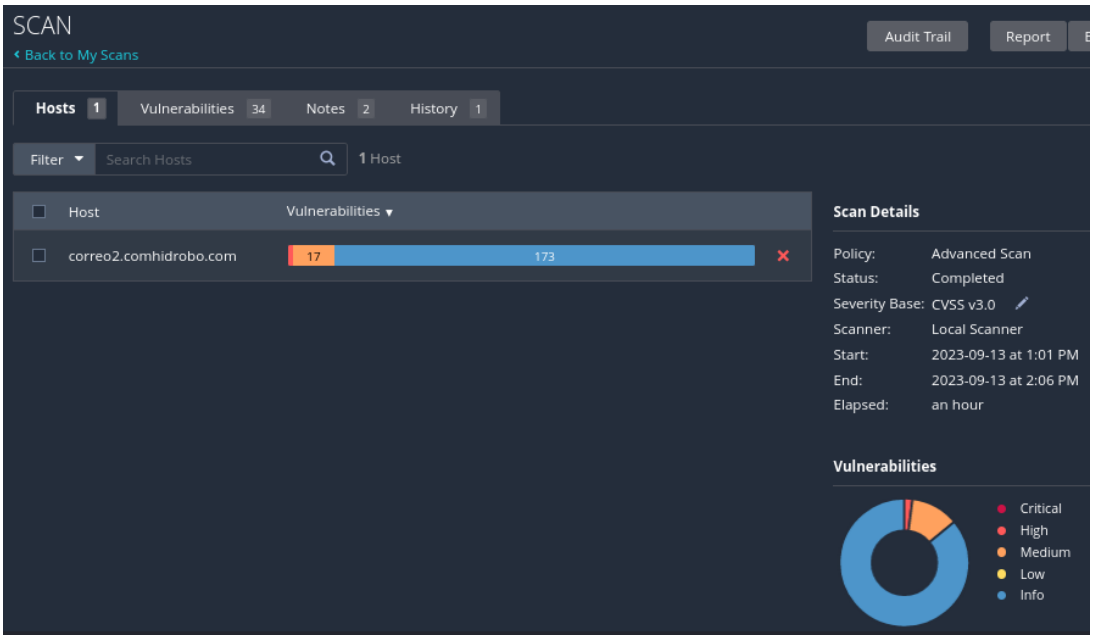


Figura 13 Finalización del escaneo. Fuente: Autor.

3.4.1 Resultados del análisis de vulnerabilidades

El informe de la Figura 14 revela la presencia de una vulnerabilidad alta, junto con 6 vulnerabilidades de nivel medio y 44 vulnerabilidades de información.

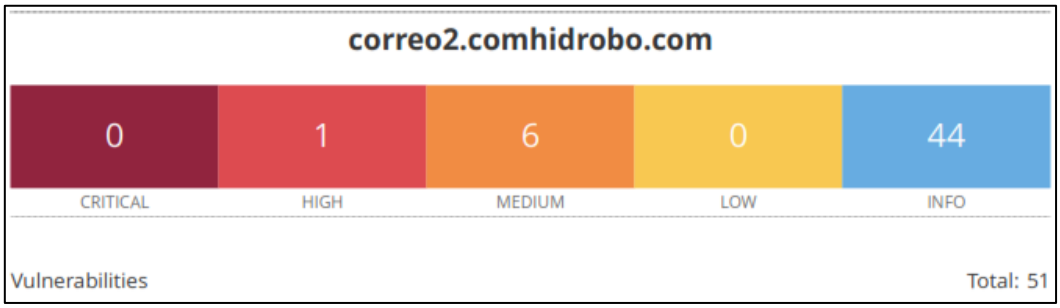


Figura 14 Resultado del escaneo. Fuente: Autor.

La estrategia adoptada en este trabajo prioriza el tratamiento de las vulnerabilidades catalogadas como altas y medias (Tabla 9), atendiendo primero aquellas que representan una amenaza crítica con un potencial significativo de impacto en la seguridad del sistema. Este enfoque garantiza una asignación inicial de recursos hacia la mitigación de los riesgos más relevantes, lo que contribuye a minimizar el tiempo dedicado a resolver falsos positivos y optimiza la precisión y eficiencia de la respuesta. La realidad de contar con recursos y tiempo limitados puede influir en esta decisión, enfocándose en las vulnerabilidades críticas para

gestionar de manera más efectiva los recursos disponibles y cumplir con los plazos establecidos de manera más efectiva.

Tabla 9 Vulnerabilidades encontradas por Nessus
Fuente: Autor

Severidad	Vulnerabilidad	Descripción
Alta	42873 - Suites de cifrado SSL de potencia media compatibles (SWEET32)	El servidor remoto presenta soporte para cifrados SSL de intensidad media, los cuales emplean una clave de al menos 64 bits y menos de 112 bits, o utilizan el algoritmo de cifrado 3DES. Es importante destacar que la vulnerabilidad de este tipo de cifrado es mayor cuando el atacante se encuentra en la misma red física.
Media	31705 - Suites de cifrado anónimo SSL compatibles	El servidor remoto permite el uso de cifrados SSL anónimos. Aunque esto facilita que un administrador configure un servicio que cifre el tráfico sin la necesidad de generar y configurar certificados SSL, no proporciona ningún medio para verificar la identidad del servidor remoto, lo que lo hace susceptible a un ataque de intermediario.
Media	51192: No se puede confiar en el certificado SSL	El certificado X.509 del servidor no es confiable, lo cual puede ocurrir cuando se rompe la cadena de confianza. Esta situación se presenta cuando la parte superior de la cadena de certificados proporcionada por el servidor no se deriva de una autoridad de certificación pública reconocida. Esto sucede cuando la parte superior de la cadena es un certificado auto firmado no reconocido o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
Media	65821 - Suites de cifrado SSL RC4	El cifrado RC4 presenta deficiencias en la generación de un flujo pseudoaleatorio de bytes,

	compatibles (Bar Mitzvah)	lo que resulta en la introducción de varios pequeños sesgos en el flujo, afectando su aleatoriedad. Cuando se cifra repetidamente texto sin formato, como sucede con las cookies HTTP, y un atacante obtiene numerosos textos cifrados, posiblemente en cantidades significativas (por ejemplo, decenas de millones), existe la posibilidad de derivar el texto sin formato.
Media	57582 - Certificado SSL auto firmado	La cadena de certificados X.509 utilizada por este servicio no cuenta con la firma de una autoridad de certificación reconocida. Esta situación compromete la efectividad del protocolo SSL, especialmente si el host remoto está en un entorno público en producción, ya que podría ser vulnerable a ataques de intermediario. Es importante tener en cuenta que este complemento no examina cadenas de certificados que finalicen en un certificado no auto firmado, pero sí firmado por una autoridad certificadora no reconocida.
Media	52633 - Memcached desprotegido	Memcached es un sistema de almacenamiento de objetos en memoria. Dado que su diseño se centra en la optimización del rendimiento, no incluye ningún mecanismo de seguridad, como la autenticación. Por lo tanto, cualquier usuario tiene la capacidad de conectarse al servidor Memcached y realizar consultas en él.

Nota: Adaptado de “Reposito de la Universidad del Bosque”, por Sandra Martínez y Gerald Tovar, 2021, Recuperado de http://repositorio.unbosque.edu.co/server/api/bitstreams/b79d7746-3685-491d-99e9-3ac87ff928fb/content Una vista más detallada, se puede observar en el **ANEXO 2**: “Reporte del Análisis de vulnerabilidades de Nessus Essentials

3.4.2 Plan de mitigación: Implementación de controles CIS en el servicio de comunicación asíncrona

Se lleva a cabo una evaluación exhaustiva del servidor de correo electrónico con el fin de identificar posibles vulnerabilidades y puntos débiles. Esta evaluación se realiza siguiendo el **ANEXO 3** del Check List de CIS Control v.8, donde se detallan los criterios específicos a considerar.

Para garantizar la seguridad del servicio de comunicación asíncrona, se hace referencia a las guías proporcionadas por CIS, las cuales se utilizan como principal marco de referencia. Se siguen las recomendaciones detalladas en estas guías para fortalecer la seguridad del servidor.

Se procede con la implementación de controles de acceso, lo que implica configurar medidas como la autenticación fuerte, la gestión de cuentas de usuario y la revisión de los permisos de acceso al servicio.

Se establecen procedimientos de monitoreo continuo para identificar y responder a eventos de seguridad en tiempo real. Se configuran alertas para detectar anomalías en el tráfico y actividades sospechosas que puedan comprometer la seguridad del sistema.

Se establece un programa de gestión de parches para garantizar que el servicio de comunicación asíncrona esté actualizado con las últimas correcciones de seguridad. Se automatiza este proceso siempre que sea posible para garantizar una respuesta rápida a nuevas amenazas.

Se desarrolla y documenta un plan de respuesta a incidentes que incluye procedimientos para la detección, notificación, mitigación y recuperación de posibles violaciones de seguridad que puedan surgir.

Se realizan auditorías periódicas para evaluar la eficacia de los controles implementados. Se ajustan y mejoran continuamente la configuración y las políticas de seguridad en respuesta a cambios en la amenaza y el entorno operativo.

Se proporciona capacitación regular a los usuarios y al personal responsable del servicio de comunicación asíncrona sobre las mejores prácticas de seguridad. Se busca concienciarlos

sobre la importancia de mantener una postura de seguridad sólida para proteger la integridad y confidencialidad de los datos.

3.5 Fase 2: Implementación de controles CIS v.8

Tras realizar el análisis de vulnerabilidades utilizando las herramientas mencionadas y al integrar la metodología MAGERIT v.3 junto con la Norma ISO/IEC 27001:2022, se identifican las vulnerabilidades más críticas que requieren mayor atención. Esto permite definir cuáles de los 20 controles CIS son aplicables a la empresa Comercial Hidrobo S.A. Los primeros seis controles se consideran básicos y deben implementarse en todo sistema o entorno, mientras que se toman en cuenta dos controles adicionales, el 7 y el 9, que están directamente relacionados con el servicio de comunicación asíncrona.

La Tabla 6 muestra los controles directamente aplicables al servicio de comunicación asíncrona. La implementación de los controles CIS en un servicio de comunicación asíncrona incluye salvaguardas específicas diseñadas para fortalecer la seguridad. Estas abordan aspectos clave de la protección de la información y contribuyen a mitigar vulnerabilidades, fortaleciendo la postura general de seguridad de la plataforma. A continuación, se presenta una descripción general de cómo estas desempeñan un papel crucial.

3.5.1 Inventario y control de activos empresariales (Control CIS 1)

Este control se enfoca en la gestión del inventario y control de activos empresariales, destacando la importancia de mantener un inventario actualizado de hardware para mejorar la seguridad y la eficiencia en la gestión de activos. Al conocer y controlar el hardware, una organización puede reducir su superficie de ataque y mejorar su capacidad para responder eficazmente a incidentes de seguridad. Se aplican diversas salvaguardas para cumplir con este control, siendo las más relevantes aquellas que directamente ayudan a mitigar vulnerabilidades. Estas se detallan en la Tabla 10.

Tabla 10 Control CIS 1
Fuente: Autor

Salvaguarda	Descripción
1.1	Establecer y mantener un inventario detallado de activos empresariales
1.2	Abordar activos no autorizados
1.3	Utilice una herramienta de descubrimiento activo

3.5.2 Inventario y Control de activos de software (CIS Control 2):

Este control se centra en la importancia de inventariar y controlar el software de una organización. La gestión adecuada del software es esencial para reducir el riesgo de exposición a amenazas y garantizar la eficacia de los controles de seguridad. Se aplican diversas salvaguardas para cumplir con este control, siendo las más destacadas aquellas que directamente ayudan a mitigar vulnerabilidades. Estas se detallan en la Tabla 11.

Tabla 11 Salvaguardas del Control CIS 2
Fuente: Autor

Salvaguarda	Descripción
2.1	Establecer y mantener un inventario detallado de activos empresariales.
2.2	Asegúrese de que el software autorizado sea actualmente compatible
2.3	Abordar el software no autorizado
2.5	Software autorizado en la lista de permitidos

3.5.3 Establecer y mantener un proceso de gestión de datos (Control CIS 3)

Este control se enfoca en la implementación de medidas para proteger los datos de la organización, lo cual implica la clasificación de datos, la encriptación y otras estrategias para garantizar la integridad, confidencialidad y disponibilidad de la información sensible. Se aplican la mayoría de las salvaguardas, a excepción de 3.6, 3.7 y 3.9, dado que no están directamente relacionadas con el servicio de comunicación asíncrona. Las salvaguardas más destacadas y que directamente contribuyen a mitigar vulnerabilidades se detallan en la Tabla 12.

Tabla 12 Salvaguardas del Control CIS 3
Fuente: Autor

Salvaguarda	Descripción
3.1	Establecer y mantener un proceso de gestión de datos.
3.2	Establecer y mantener un inventario de datos.
3.3	Configuración de listas de control de acceso a datos (listas blancas).
3.4	Hacer cumplir la retención de datos.
3.5	Eliminar datos de forma segura.

3.8	Flujos de datos de documentos.
3.10	Cifrar datos confidenciales en tránsito.
3.11	Cifrar datos confidenciales en reposo.
3.12	Segmentar el procesamiento y almacenamiento de datos según la sensibilidad.
3.13	Implementar una solución de prevención de pérdida de datos.
3.14	Registrar acceso a datos confidenciales.

3.5.4 Configuración segura de activos y software empresariales (Control CIS 4)

La configuración segura es esencial para reducir la superficie de ataque y mitigar los riesgos asociados con configuraciones inseguras que podrían ser explotadas por amenazas. La mayoría de las salvaguardas se aplican, con excepción de 4.10 y 4.11, ya que no están directamente relacionadas con el servicio de comunicación asíncrona. Las salvaguardas más destacadas que contribuyen directamente a mitigar vulnerabilidades se muestran en la Tabla 13.

Tabla 13 Salvaguardas del Control CIS 4
Fuente: Autor

Salvaguarda	Descripción
4.1	Establecer y mantener un proceso de configuración seguro.
4.2	Establecer y mantener un proceso de configuración seguro para la infraestructura de red.
4.3	Configuración del bloqueo automático de sesiones en activos empresariales.
4.4	Implementar y administrar un firewall en servidores
4.5	Implementar y administrar un firewall en dispositivos de usuario final.
4.6	Administre de forma segura los activos y el software empresarial.
4.7	Administrar cuentas predeterminadas en software y activos empresariales.
4.8	Desinstalar o deshabilitar servicios innecesarios en software y activos empresariales.
4.9	Configuración servidores DNS confiables en activos empresariales

3.5.5 Administración de cuentas (Control CIS 5)

Se enfoca en la administración efectiva de cuentas de usuario para garantizar la seguridad de los sistemas y datos. La implementación de prácticas sólidas en la gestión de cuentas es esencial para prevenir accesos no autorizados y proteger la integridad de la información. Todas las salvaguardas se aplican, siendo las más destacadas y que ayudan directamente a mitigar vulnerabilidades las que se enlistan en la Tabla 14.

Tabla 14 Salvaguardas del Control CIS 5
Fuente: Autor

Salvaguarda	Descripción
5.1	Establecer y mantener un inventario de cuentas.
5.2	Utilice contraseñas únicas
5.3	Deshabilitar cuentas inactivas
5.4	Restringir los privilegios de administrador a dedicados

3.5.6 Gestión de control de acceso (Control CIS 6)

Se enfoca en la gestión integral del control de acceso para garantizar que los usuarios tengan los privilegios adecuados y minimizar el riesgo de acceso no autorizado. La implementación de políticas y prácticas efectivas en este control es esencial para mantener la seguridad de los sistemas y la confidencialidad de la información. Todas las salvaguardas de la Tabla 15 se aplican.

Tabla 15 Salvaguardas del Control CIS 6
Fuente: Autor

Salvaguarda	Descripción
6.1	Establecer un proceso de concesión de acceso.
6.2	Establecer un proceso de revocación de acceso.
6.3	Requerir MFA para aplicaciones expuestas externamente.
6.4	Requerir MFA para acceso remoto a la red
6.5	Requerir MFA para acceso administrativo
6.6	Establecer y mantener un inventario de sistemas de autenticación y autorización.
6.7	Centralizar el control de acceso

6.8	Control de acceso basado en roles

3.5.7 Gestión continua de vulnerabilidades (Control CIS 7)

Se centra en identificar, evaluar y abordar de manera proactiva las posibles debilidades en los sistemas y aplicaciones. La implementación de este control es esencial para reducir la ventana de exposición a amenazas y minimizar el riesgo de explotación de vulnerabilidades. Todas las salvaguardas de la Tabla 16 se aplican.

Tabla 16 Salvaguardas del Control CIS 7
Fuente: Autor

Salvaguarda	Descripción
7.1	Establecer y mantener un proceso de gestión de vulnerabilidades.
7.2	Establecer y mantener un proceso de remediación
7.3	Realizar la gestión automatizada de parches del sistema operativo.
7.4	Realizar la gestión automatizada de parches de aplicaciones.
7.5	Realizar análisis automatizados de vulnerabilidades internas.
7.6	Realizar análisis de vulnerabilidad automatizados de objetos expuestos externamente.
7.7	Remediar vulnerabilidades detectadas.

3.5.8 Protecciones de correo electrónico y navegador web (Control CIS 9)

Este control se enfoca en implementar medidas de seguridad específicas para proteger el correo electrónico y los navegadores web, dos vectores críticos que son frecuentemente aprovechados por amenazas cibernéticas. La implementación de este control es fundamental para reducir el riesgo de ataques dirigidos a través de estos canales. Todas las salvaguardas especificadas se aplican (Tabla 17).

Tabla 17 Salvaguardas del Control CIS 9
Fuente: Autor

Salvaguarda	Descripción
9.1	Garantizar el uso únicamente de navegadores y clientes de correo electrónico totalmente compatibles.
9.2	Utilice servicios de filtrado DNS.
9.3	Mantener y aplicar filtros de URL basados en red.

9.4	Restringir navegadores y correos electrónicos innecesarios o no autorizados.
9.5	Implementar DMARC.
9.6	Bloquear tipos de archivos innecesarios.
9.7	Implementar y mantener protecciones antimalware del servidor de correo electrónico.

Una vista más detallada de lo especificado, se puede observar en el **ANEXO 4**: Informe de controles implementados.

3.6 Fase 3: Implementación metodología MAGERIT v3

La integración de la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y la norma ISO (Organización Internacional de Estandarización) es esencial para asegurar un enfoque completo en la seguridad de la información en un entorno de comunicación asincrónica. Al combinar estos marcos de referencia, se establece un marco sólido que aborda tanto la gestión de riesgos específica como los estándares internacionales reconocidos.

Esta fusión fortalece la postura de seguridad, proporciona una gestión de riesgos más exhaustiva y demuestra el compromiso con estándares internacionales establecidos. Esto es crucial para garantizar la confidencialidad, integridad y disponibilidad de la información en un contexto de comunicación asincrónica (Acosta Nexar, 2018).

La integración de la metodología MAGERIT en nuestro enfoque de gestión de riesgos se ha llevado a cabo de manera efectiva a través del uso de la herramienta PILAR. Lo que distingue a PILAR es su alineación específica con los principios y procesos de MAGERIT, lo que genera una sinergia única entre la metodología y su implementación práctica. En este sentido, la utilización de PILAR no solo implica la aplicación de la metodología, sino que también refleja un compromiso estratégico para aprovechar al máximo las capacidades de MAGERIT en la evaluación y mitigación de riesgos, especialmente en el contexto de la seguridad de la información en servicios de comunicación asincrónica, como el correo electrónico (Hernández, 2019). Para la implementación del método MAGERIT se contemplan las fases detalladas en la Tabla 18.

Tabla 18 Fases de la metodología MAGERIT
Fuente: Autor

N°	Fases
1	Caracterización de los activos
2	Caracterización de las amenazas
3	Evaluación de las salvaguardas

Después de completar el análisis con el método MAGERIT, se procede a ingresar los datos en la herramienta PILAR. Esta herramienta cuenta con una biblioteca que facilita la evaluación de la seguridad informática mediante una puntuación, lo que proporciona una visión clara de la situación actual. Posteriormente, se elaboran recomendaciones para el departamento de sistemas de Comercial Hidrobo.

La herramienta PILAR opera con dimensiones clave para la seguridad informática, que se detallan en la Tabla 19. Estas dimensiones son fundamentales para calcular el impacto y el riesgo acumulado, potencial y residual.

Tabla 19 Dimensiones del método MAGERIT v3
Fuente: Autor

Dimensiones
Confidencialidad
Integridad
Disponibilidad
Autenticidad
Trazabilidad
Datos Personales

Se emplea la herramienta PILAR para llevar a cabo el análisis y la gestión de riesgos, como se ilustra en la Figura 15. Luego, se procede a ingresar los datos correspondientes al proyecto (Figura 16).

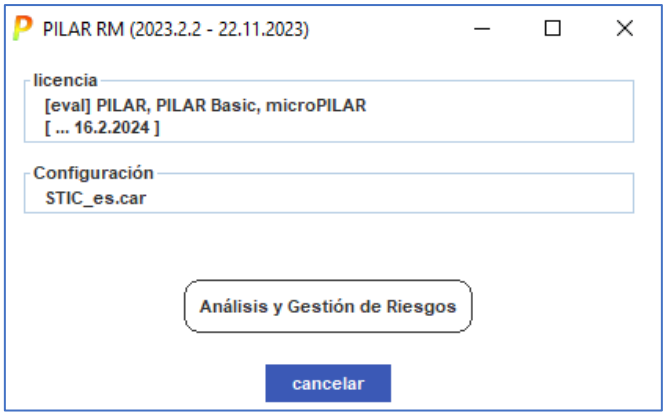


Figura 15 Pantalla principal herramienta PILAR. Fuente: Autor.

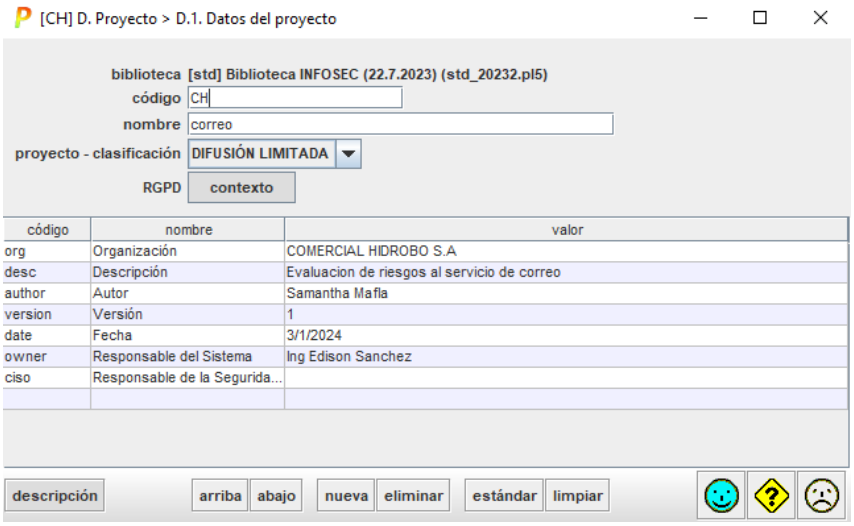


Figura 16 Datos del proyecto. Fuente: Autor.

3.6.1 Determinación de activos

Los activos se definen como cualquier información que una organización valore y desee proteger para asegurar su confidencialidad, integridad y disponibilidad. La norma ISO clasifica estos activos de la siguiente manera, como se muestra en la Tabla 20.

Tabla 20 Clasificación de activos.
Fuente: Actor

Clasificación de Activos	Descripción
Información	Bases de datos, documentación, manuales, procedimientos, etc.
Documentos físicos	Documentos impresos en papel que se almacenan en archivo como contratos, documentos legales entre otros.
Software	Todo sistema que se use dentro de la empresa.
Hardware	Todos los equipos de tecnología como computadores, servidores, etc.
Recurso Humano	Todo el personal que colabora en la organización.
Servicios	Servicios que apoyan a la empresa para su funcionamiento como servicios básicos, internet, etc.

En la empresa, varios trabajadores son responsables de diferentes activos, y cada activo manipulado está asociado al cargo que ocupa. Por ende, no todos tienen el mismo nivel de seguridad aplicable, por lo que es necesario analizar cada uno de ellos. Centrándose en el proyecto actual, el objetivo es analizar los activos del servicio de comunicación asincrónica, los cuales se detallan en la Tabla 21. En la Figura 17 se detalla el ingreso de los activos en la herramienta PILAR.

Tabla 21 Activos de la empresa Comercial Hidrobo S.A
Fuente: Autor

Tipo de activo	**Activo**
Datos	Bases de datos que almacenan información de usuarios, correos electrónicos y metadatos. Registro de eventos
Software	Servidor de correo entrante IMAP Servidor de correo saliente SMTP Servidores de almacenamiento de correo (como servidores de buzones). Sistema operativo en que está alojado el servidor de correo. Antivirus
Hardware	Servidor físico Equipos PC de usuarios finales Laptops Switches Router Rack Firewall
Redes de Comunicación	Red de datos Red Inalámbrica Internet
Equipamiento auxiliar	Ups Fibra Óptica
Instalaciones	Departamento de Sistemas de Comercial Hidrobo
Personal	Miembros del departamento de sistemas

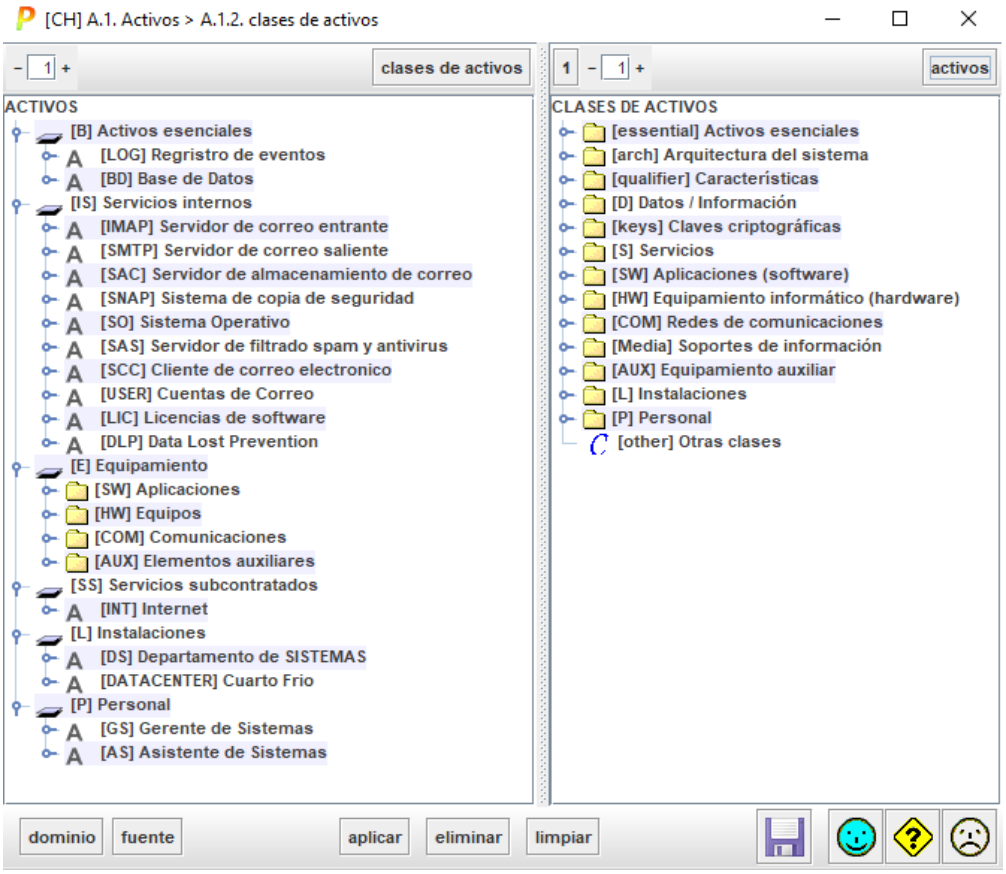
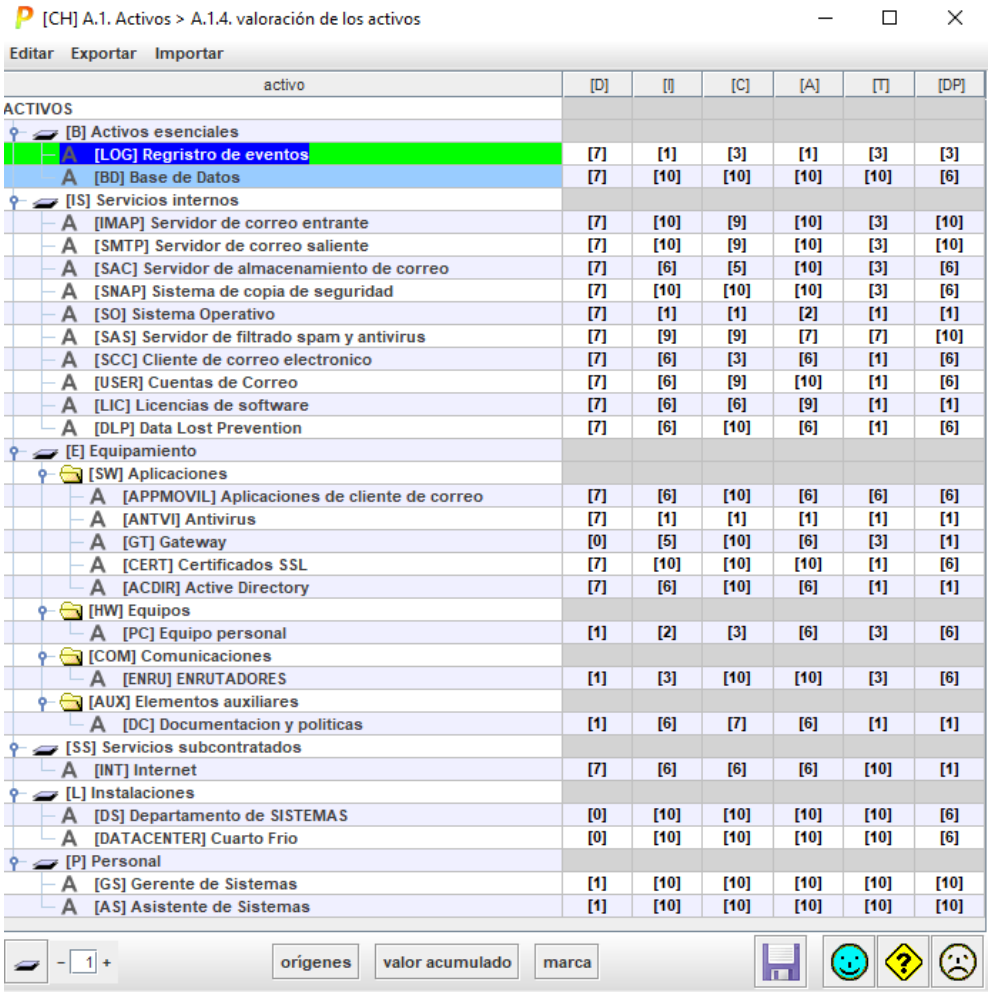


Figura 17 Activos del servicio de comunicación asíncrona. Fuente: Autor.

3.6.2 Valoración de Activos

Para establecer el valor de cada activo, es fundamental comprender minuciosamente el proceso que se va a evaluar. Esto implica recopilar información detallada de la documentación existente sobre el proceso en cuestión, así como interactuar directamente con las personas responsables del proceso y aquellas que lo útil an regularmente. En la Figura 18 se presenta la evaluación de cada activo en términos de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad y datos personales.



[CH] A.1. Activos > A.1.4. valoración de los activos

Editar Exportar Importar

activo	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS						
[B] Activos esenciales						
[LOG] Registro de eventos	[7]	[1]	[3]	[1]	[3]	[3]
[BD] Base de Datos	[7]	[10]	[10]	[10]	[10]	[6]
[IS] Servicios internos						
[IMAP] Servidor de correo entrante	[7]	[10]	[9]	[10]	[3]	[10]
[SMTP] Servidor de correo saliente	[7]	[10]	[9]	[10]	[3]	[10]
[SAC] Servidor de almacenamiento de correo	[7]	[6]	[5]	[10]	[3]	[6]
[SNAP] Sistema de copia de seguridad	[7]	[10]	[10]	[10]	[3]	[6]
[SO] Sistema Operativo	[7]	[1]	[1]	[2]	[1]	[1]
[SAS] Servidor de filtrado spam y antivirus	[7]	[9]	[9]	[7]	[7]	[10]
[SCC] Cliente de correo electronico	[7]	[6]	[3]	[6]	[1]	[6]
[USER] Cuentas de Correo	[7]	[6]	[9]	[10]	[1]	[6]
[LIC] Licencias de software	[7]	[6]	[6]	[9]	[1]	[1]
[DLP] Data Lost Prevention	[7]	[6]	[10]	[6]	[1]	[6]
[E] Equipamiento						
[SW] Aplicaciones						
[APPMOVIL] Aplicaciones de cliente de correo	[7]	[6]	[10]	[6]	[6]	[6]
[ANTVI] Antivirus	[7]	[1]	[1]	[1]	[1]	[1]
[GT] Gateway	[0]	[5]	[10]	[6]	[3]	[1]
[CERT] Certificados SSL	[7]	[10]	[10]	[10]	[1]	[6]
[ACDIR] Active Directory	[7]	[6]	[10]	[6]	[1]	[1]
[HW] Equipos						
[PC] Equipo personal	[1]	[2]	[3]	[6]	[3]	[6]
[COM] Comunicaciones						
[ENRU] ENRUTADORES	[1]	[3]	[10]	[10]	[3]	[6]
[AUX] Elementos auxiliares						
[DC] Documentacion y politicas	[1]	[6]	[7]	[6]	[1]	[1]
[SS] Servicios subcontratados						
[INT] Internet	[7]	[6]	[6]	[6]	[10]	[1]
[L] Instalaciones						
[DS] Departamento de SISTEMAS	[0]	[10]	[10]	[10]	[10]	[6]
[DATACENTER] Cuarto Frio	[0]	[10]	[10]	[10]	[10]	[6]
[P] Personal						
[GS] Gerente de Sistemas	[1]	[10]	[10]	[10]	[10]	[10]
[AS] Asistente de Sistemas	[1]	[10]	[10]	[10]	[10]	[10]

- 1 + orígenes valor acumulado marca

Figura 18 Valoración de activos de servicio de comunicación asíncrona. Fuente: Autor

La Figura 19 presenta un gráfico que ilustra el valor del dominio del servicio de comunicación asincrónica. Por otro lado, la Figura 20 muestra una representación gráfica de los activos de este servicio, donde se asignan distintos niveles de valor a cada uno de ellos.

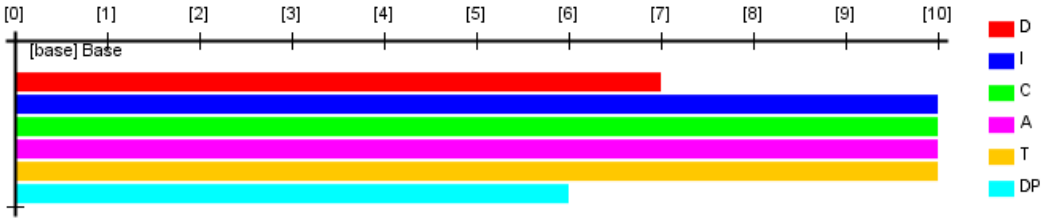


Figura 19 Valoración de dominio del servicio de comunicación asíncrona. Fuente: Autor.

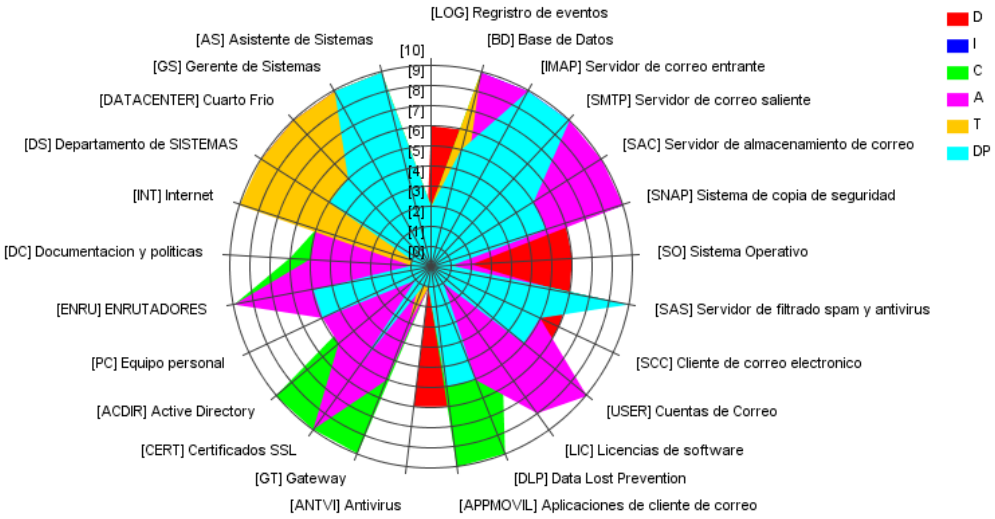


Figura 20 Grafica valor/activos. Fuente: Autor.

3.6.3 Identificación de amenazas

Para identificar las amenazas que podrían afectar a los activos de la organización, se requiere verificar la existencia de políticas de seguridad específicas para el servicio de comunicación asincrónica bajo evaluación. Estas amenazas pueden clasificarse en dos categorías: intencionales, que son identificadas y cuentan con un plan de acción correspondiente, y fortuitas, que son incidentes imprevistos.

Tras la valoración de los activos en la herramienta PILAR, se generan asociaciones con posibles amenazas para cada uno de ellos, como se visualiza en la Figura 21.

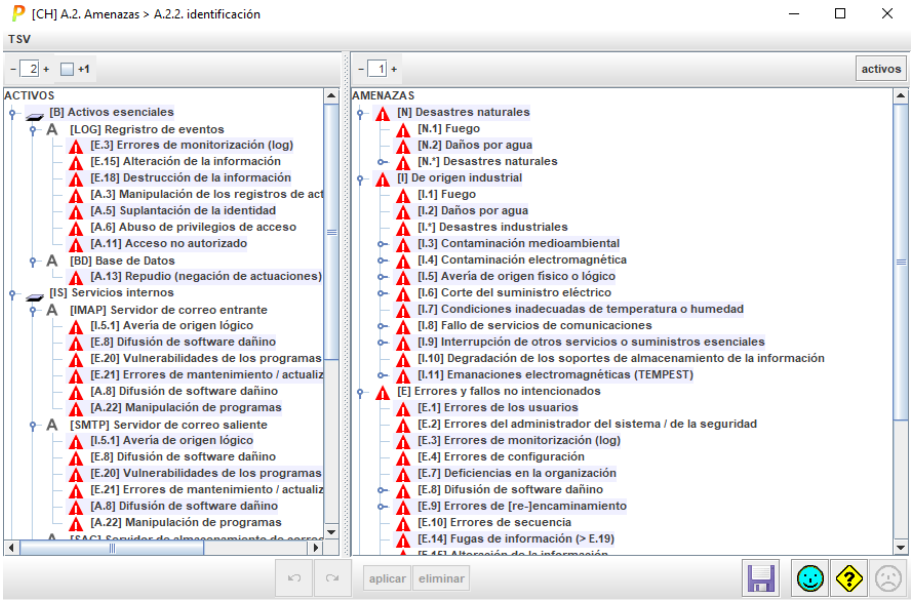


Figura 21 Amenazas del servicio de comunicación asíncrona. Fuente: Autor

3.6.4 Valoración de amenazas

Los aspectos necesarios para la valoración de amenazas incluyen la probabilidad de ocurrencia, que representa la frecuencia con la que una amenaza puede repetirse, como se detalla en la Tabla 22, y el porcentaje de degradación, que indica el grado de deterioro o daño experimentado después de un incidente. Para calcular adecuadamente la valoración de la amenaza, es crucial distinguir entre amenazas intencionales y fortuitas, y el porcentaje de degradación se determina en relación con la dimensión afectada, valorada del 1% al 100% (Quirola, 2019).

Tabla 22 Probabilidad de ocurrencia
Fuente: Autor

Valoración	Frecuencia
100	Diariamente
10	Mensualmente
1	Normal
1/10	Cada década
1/100	Cada siglo

La asignación de valoraciones a las amenazas por parte de PILAR se verifica en la Figura 22, mientras que en la Figura 23 se puede apreciar la probabilidad de ocurrencia en la columna de frecuencia.

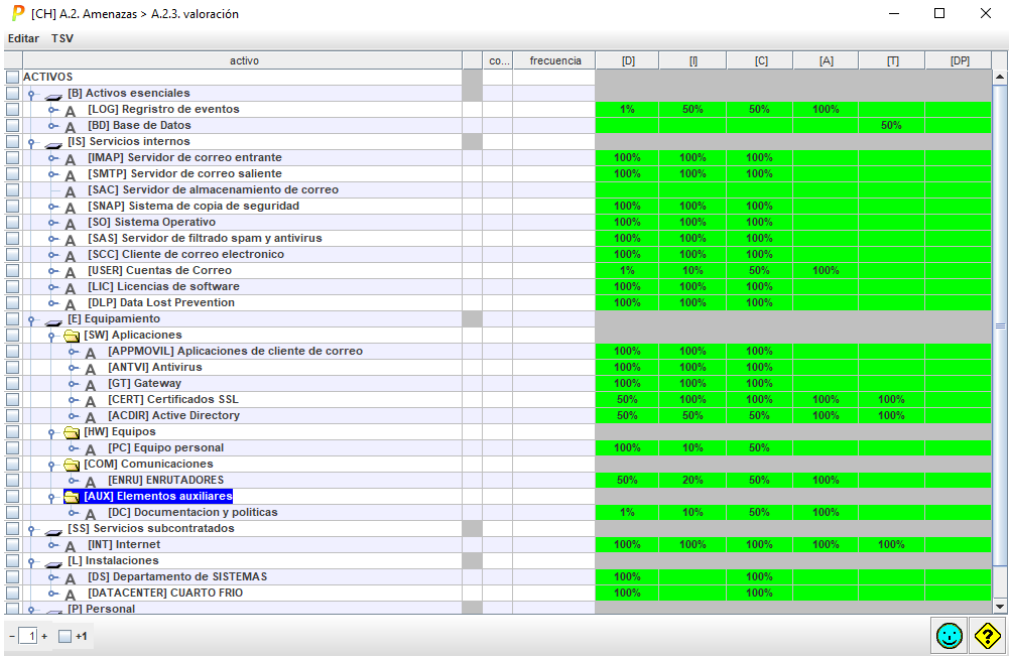
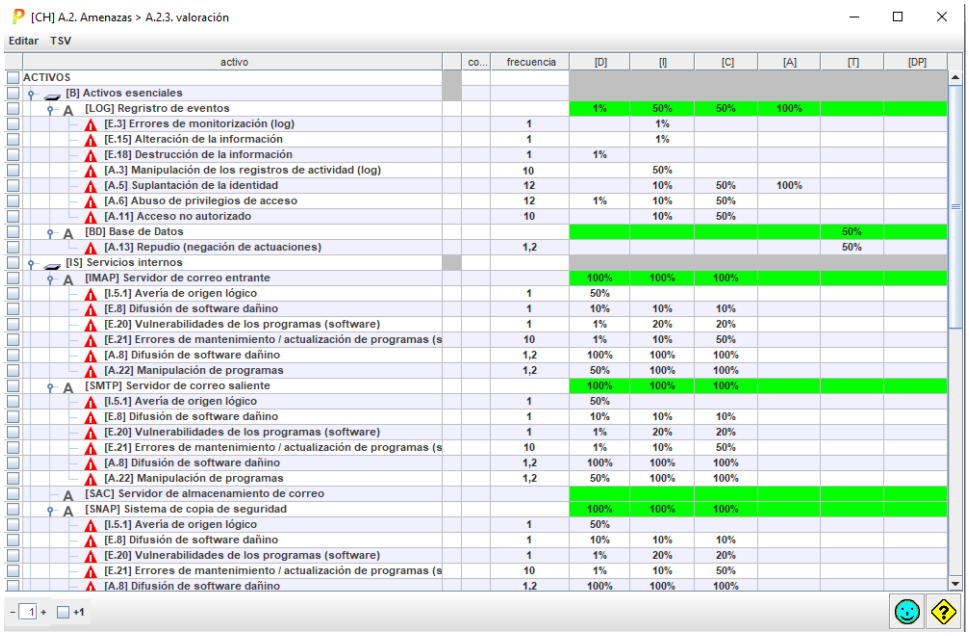


Figura 22 Amenazas del servicio de comunicación asíncrono. Fuente: Autor



activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[DP]
ACTIVOS								
[B] Activos esenciales								
[LOG] Registro de eventos			1%	50%	50%	100%		
[E.3] Errores de monitorización (log)		1		1%				
[E.15] Alteración de la información		1		1%				
[E.18] Destrucción de la información		1	1%					
[A.3] Manipulación de los registros de actividad (log)		10		50%				
[A.5] Suplantación de la identidad		12		10%	50%	100%		
[A.6] Abuso de privilegios de acceso		12	1%	10%	50%			
[A.11] Acceso no autorizado		10		10%	50%			
[BD] Base de Datos							50%	
[A.13] Repudio (negación de actuaciones)		1,2					50%	
[IS] Servicios internos								
[IMAP] Servidor de correo entrante			100%	100%	100%			
[I.5.1] Avería de origen lógico		1	50%					
[E.8] Difusión de software dañino		1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programas (s		10	1%	10%	50%			
[A.8] Difusión de software dañino		1,2	100%	100%	100%			
[A.22] Manipulación de programas		1,2	50%	100%	100%			
[SMTP] Servidor de correo saliente			100%	100%	100%			
[I.5.1] Avería de origen lógico		1	50%					
[E.8] Difusión de software dañino		1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programas (s		10	1%	10%	50%			
[A.8] Difusión de software dañino		1,2	100%	100%	100%			
[A.22] Manipulación de programas		1,2	50%	100%	100%			
[SAC] Servidor de almacenamiento de correo								
[SNAP] Sistema de copia de seguridad			100%	100%	100%			
[I.5.1] Avería de origen lógico		1	50%					
[E.8] Difusión de software dañino		1	10%	10%	10%			
[E.20] Vulnerabilidades de los programas (software)		1	1%	20%	20%			
[E.21] Errores de mantenimiento / actualización de programas (s		10	1%	10%	50%			
[A.8] Difusión de software dañino		1,2	100%	100%	100%			

Figura 23 Amenazas y probabilidad de ocurrencia. Fuente: Autor

3.6.5 Estimación de impacto

El impacto de las amenazas se refiere al daño resultante cuando estas se materializan. La estimación de este impacto involucra diversos factores, tal como se detalla en la Tabla 23. Según (Guaman, 2019) los efectos pueden dar lugar a repercusiones tanto cualitativas como cuantitativas, como pérdidas financieras o un deterioro en la percepción del cliente hacia la organización, entre otros posibles resultados. Es importante establecer una relación entre los efectos de los riesgos identificados y las medidas de protección necesarias. Además, se debe considerar la frecuencia con la que ocurren las amenazas, dado que la ocurrencia simultánea de múltiples amenazas podría provocar pérdidas y daños significativos para la organización.

Tabla 23 Factores de estimación
Fuente: Autor

Amenazas
Afecta totalmente a un activo.
Afecta elementos críticos de un activo.
Afecta de manera temporal o permanente.

3.6.6 Impacto acumulado

El impacto total puede determinarse al considerar cada activo, cada amenaza y su valoración respectiva. Este cálculo se fundamenta en la degradación y el valor acumulado, de modo que a medida que la degradación aumenta, también lo hace el impacto acumulado. Conocer el impacto acumulado resulta fundamental para identificar las salvaguardas que deben implementarse en la organización. En la Figura 24 se presenta el impacto acumulado según lo

calculado en la herramienta PILAR. La gráfica representada en la Figura 25, muestra el riesgo acumulado, donde el color rojo indica el impacto actual del riesgo en el servicio, mientras que el color azul muestra el nivel recomendado por PILAR.

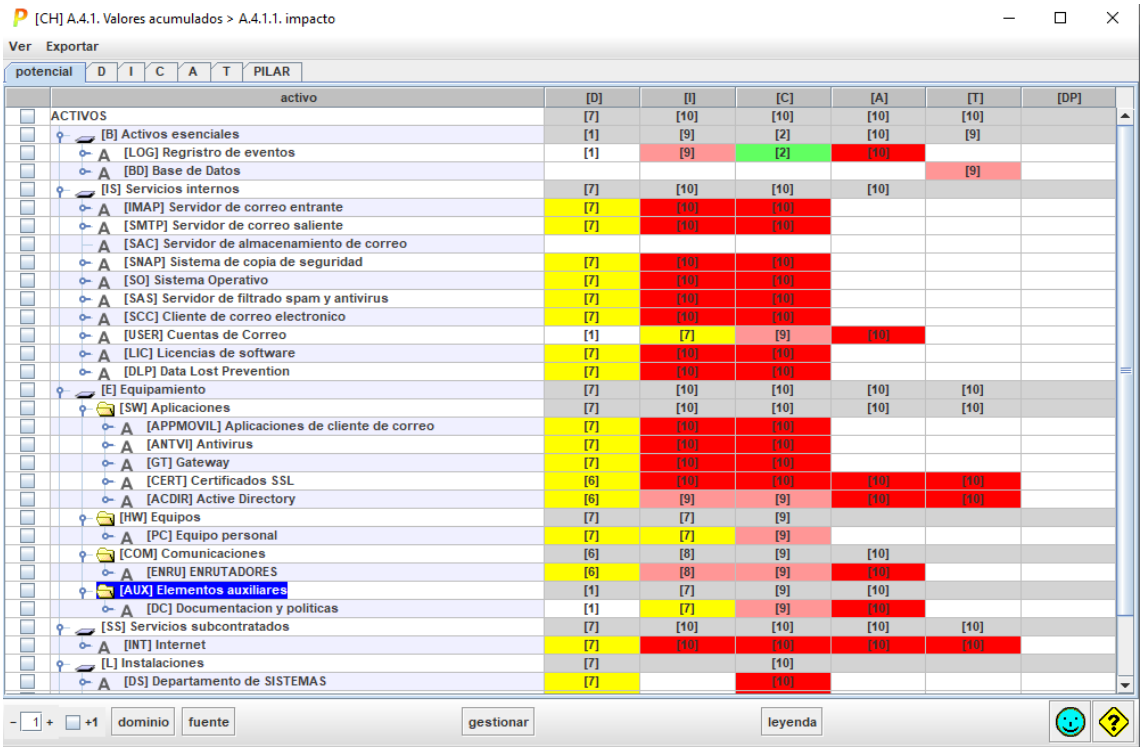


Figura 24 Impacto acumulado del servicio de comunicación asíncrona. Fuente: Autor

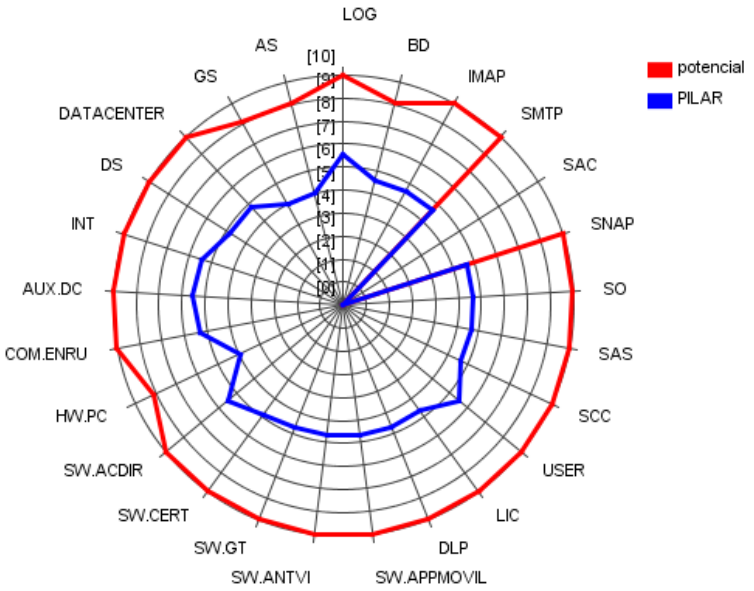


Figura 25 Situación actual del impacto acumulado del servicio de comunicación asíncrona. Fuente: Autor.

3.6.7 Riesgo acumulado e impacto repercutido

En la Figura 26 se presenta el riesgo acumulado del servicio de comunicación asincrónica. Este valor repercute en la ocurrencia de posibles implicaciones derivadas de incidentes técnicos en el sistema de información, determinado según el valor de los activos. Asimismo, en la Figura 27 se visualiza el riesgo acumulado actual del servicio, donde el color x representa el nivel de riesgo actual, mientras que el color y representa el nivel recomendado por PILAR. Por otro lado, en la Figura 28 se muestra el riesgo acumulado por dimensión, destacando que lo recomendado por la herramienta PILAR está representado en color x, mientras que lo actualmente observado supera lo recomendado.

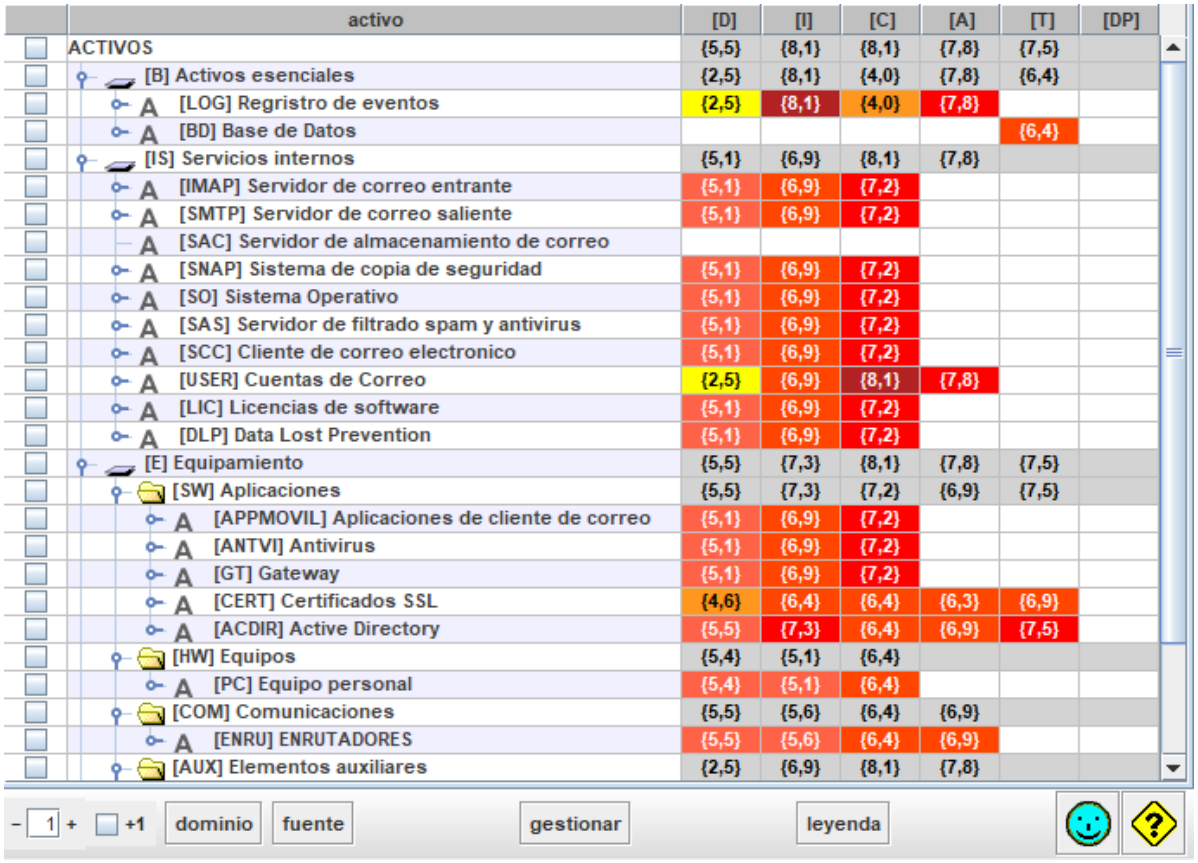


Figura 26 Riesgo acumulado del servicio de comunicación asíncrona. Fuente:Autor

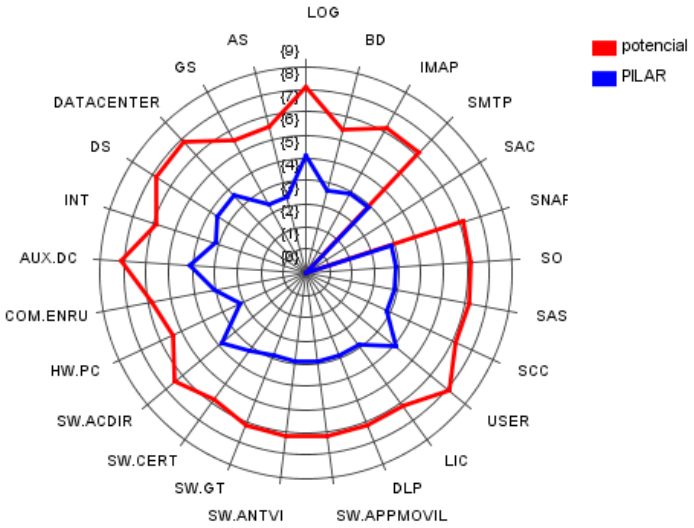


Figura 27 Riesgo acumulado del servicio de comunicación asíncrona Fuente: Autor

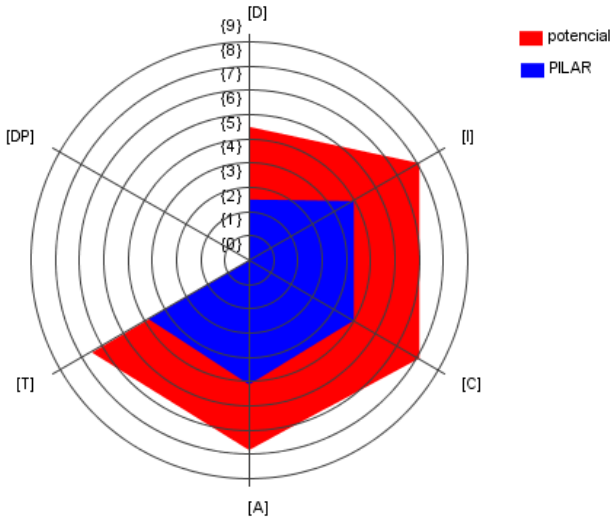


Figura 28 Riesgo acumulado/dimensión Fuente: Autor

Basándose en los resultados obtenidos del análisis, resulta crucial mitigar los riesgos existentes, dado que el valor encontrado es considerablemente alto en comparación con lo sugerido por la metodología. De esta forma, se asegura la preservación de la seguridad de la información.

CAPITULO IV

RESULTADOS

4.1 Mitigación de vulnerabilidades

En esta sección, se verifica la efectividad de las medidas tomadas para mitigar las vulnerabilidades identificadas durante el análisis previo. Las acciones incluyen la implementación de los controles CIS y diversas configuraciones destinadas a reforzar la seguridad del servicio de comunicación asíncrona (Cabezas, 2022).

La Tabla 24 enumera las vulnerabilidades identificadas junto con las medidas de mitigación correspondientes. La información contenida se basa en los resultados del escaneo realizado por la herramienta Nessus. Esta herramienta dispone de una extensa biblioteca de vulnerabilidades que ofrece orientación sobre cómo abordar cada una de las vulnerabilidades detectadas.

Tabla 24 Vulnerabilidades SSL
Fuente: Autor

CIFRADO SSL	
Vulnerabilidad	**Mitigación**
42873 - Suites de cifrado SSL de potencia media compatibles (SWEET32)	Aplicación del control CIS 3 y la salvaguarda 11. Configuración de archivos ssl.conf.
31705 - Suites de cifrado anónimo SSL compatibles	Configuración de archivos ssl.conf.
51192: No se puede confiar en el certificado SSL	Compra de un certificado SSL/TLS 1.2 a una entidad certificadora.
65821 - Suites de cifrado SSL RC4 compatibles (Bar Mitzvah)	Compra de un certificado SSL/TLS 1.2 a una entidad certificadora.
57582 - Certificado SSL auto firmado	Compra de un certificado SSL/TLS 1.2 a una entidad certificadora.

La Tabla 25 se genera a partir de los resultados obtenidos del escaneo de vulnerabilidades utilizando el plugin de Tenable. Es crucial destacar que Tenable incorpora posibles soluciones para abordar las vulnerabilidades identificadas durante el escaneo (Tenable, Tenable Plugins, 2018).

Tabla 25 Vulnerabilidad MEMCACHED
Fuente: Autor

MEMCACHED	
Vulnerabilidad	**Mitigación**
52633 - Memcached desprotegido	Configuración en el firewall que el puerto de esta comunicación este restringido para usuarios autorizados.

Para comprobar la efectividad de la aplicación del control 3, salvaguarda 11, con respecto a la vulnerabilidad del certificado SSL, se presenta en la Figura 29 una captura de la configuración del archivo zmssl.conf. Esta configuración se utiliza para prevenir la explotación de la vulnerabilidad. El archivo contiene los ajustes de SSL destinados al servidor web Apache, específicamente para el módulo de seguridad. Su propósito es garantizar la seguridad de la comunicación entre el navegador web y el servidor Apache.

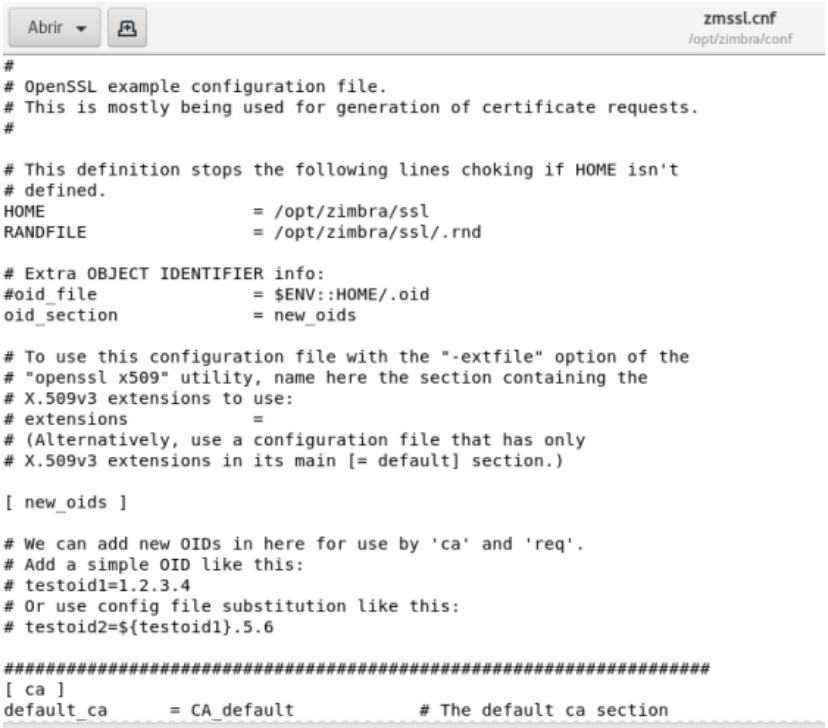


Figura 29 Archivo de configuración zmssl.conf
Fuente: Autor

Para comenzar con la instalación del certificado, primero se generan los archivos .crs y .key desde el servidor como se muestran en la Figura 30. Una vez descargados los archivos .crt desde la entidad certificadora, se colocan todos los archivos en la dirección específica para los certificados SSL en ZIMBRA (/opt/zimbra/ssl/zimbra/comercial).

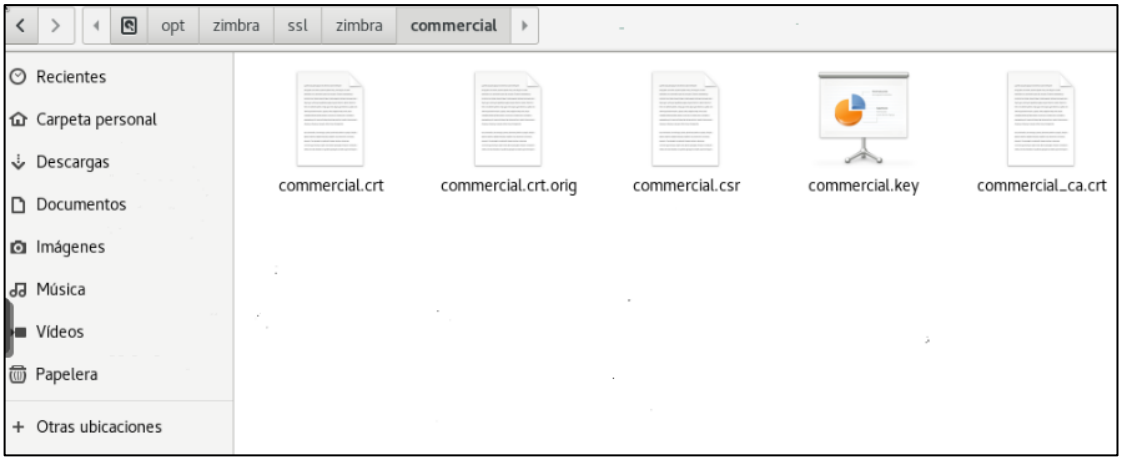


Figura 30 Archivos de configuración del certificado SSL/TLS
Fuente: Autor

En la Figura 31 se muestra el uso de la función que despliega los archivos obtenidos desde la certificadora, los mismos que finalizan la instalación del certificado.

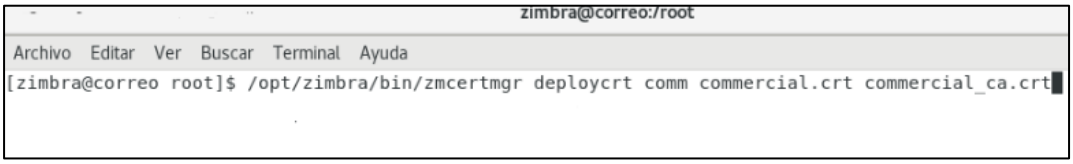


Figura 31 Comando de instalación del certificado SSL Fuente: Autor

En la Figura 32 se verifica el antes y después de haber aplicado los controles CIS 3 y 4 para una conexión segura con el servicio de comunicación asíncrona. Mitigando las dos vulnerabilidades encontradas en el análisis (31705 - Suites de cifrado anónimo SSL compatibles, 51192: No se puede confiar en el certificado SSL y 57582 - Certificado SSL auto firmado).

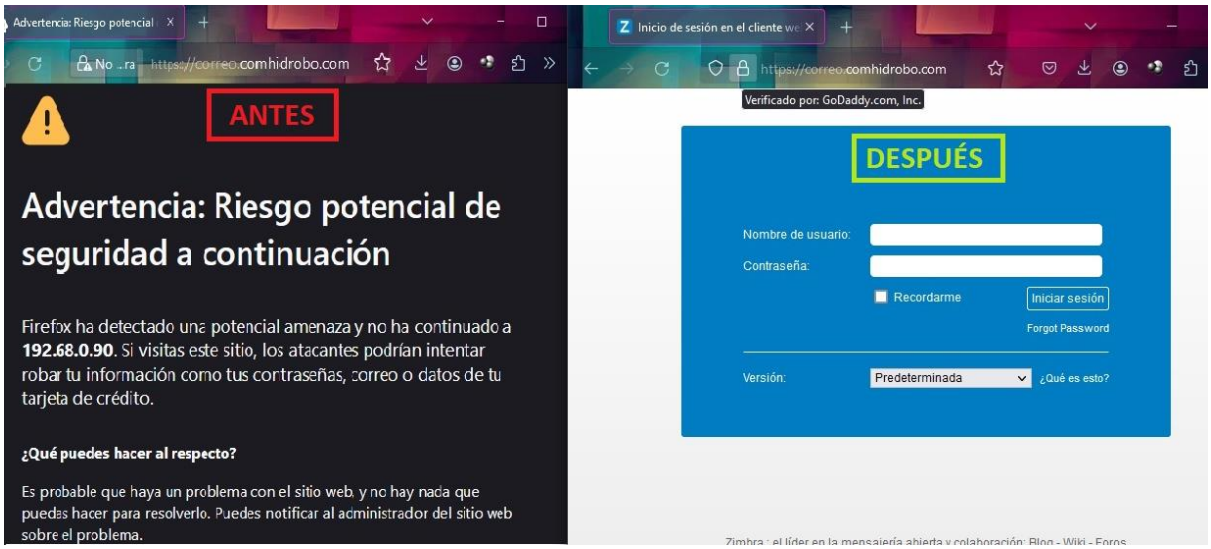


Figura 32 Verificación del certificado SSL. Fuente: Autor

La mitigación de la vulnerabilidad de Memcached se ilustra en la Figura 33. Implica la implementación de medidas de seguridad adecuadas, y una de las formas efectivas de lograrlo es a través de la configuración directa en el archivo de configuración del servicio. Esto

considera restringir la comunicación del puerto del servicio Memcached únicamente a usuarios autorizados. En la línea “OPTIONS” se coloca la lista de las IP que pueden comunicarse con este servicio.

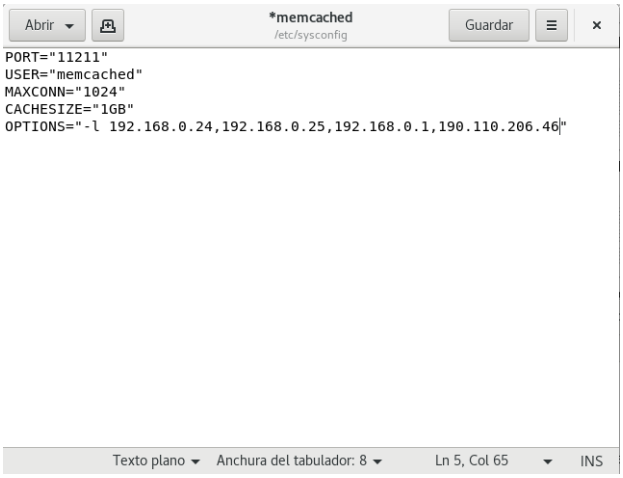


Figura 32 Configuración Memcached. Fuente: Autor

4.2 Métrica de evaluación

La métrica evaluar el impacto de las acciones de mitigación aplicadas en este estudio consiste en comparar la actividad de antispam/antivirus diariamente por el servidor antes y después de la implementación de las salvaguardas.

La Figura 34 exhibe el pico máximo de eventos registrados, ocurrido en noviembre de 2023, previo a la aplicación de las salvaguardas. Tras implementar estas medidas, se ha observado una notable disminución en la cantidad de registros. Actualmente, se monitorea diariamente para garantizar que el registro de actividades se mantenga en un rango mínimo de 1 a 10, lo cual es considerado normal para el servidor.

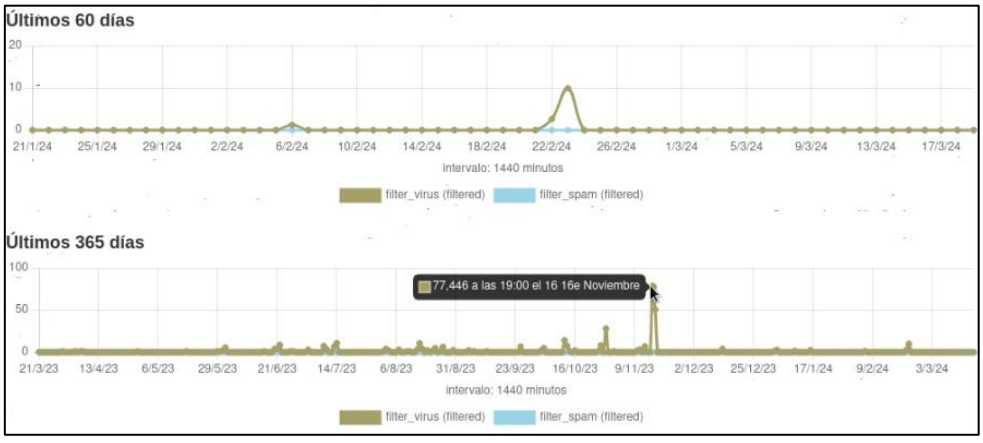


Figura 33 Actividad antispam/antivirus. Fuente: Autor

En la Figura 35 se aprecia la cantidad de registros de actividad el 29 de enero de 2024, después de haber implementado las salvaguardas. Este número se ha establecido como un nuevo rango máximo.

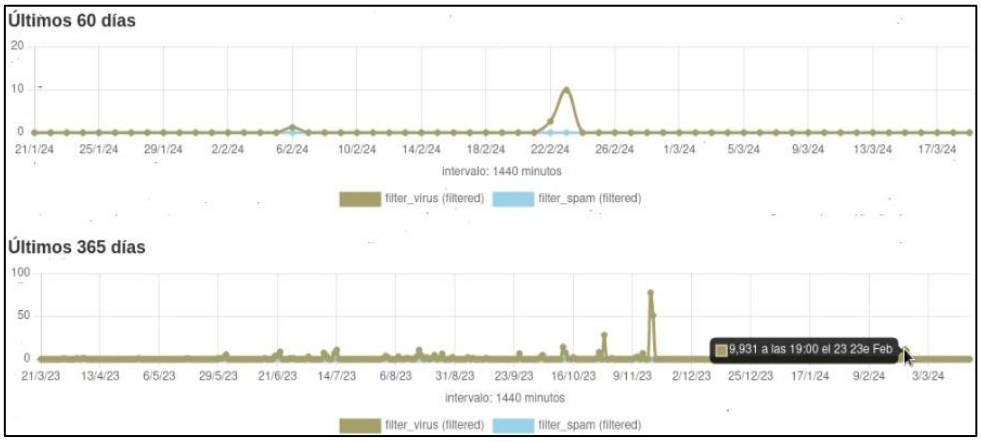


Figura 34 Actividad antispam/antivirus después de la aplicación de las salvaguardas. Fuente: Autor

Desde el año 2024, tras la implementación de las salvaguardas, se ha registrado una disminución drástica en la cantidad de eventos, como se puede observar en la Figura 36.

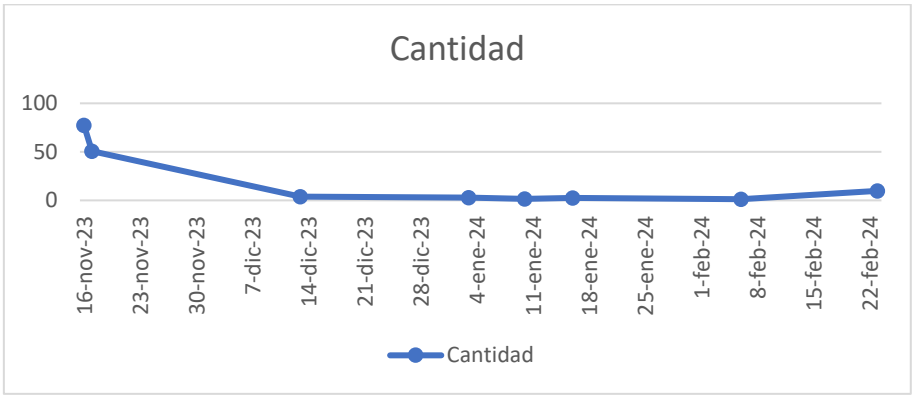


Figura 35 Grafica de eventos antispam/antivirus. Fuente: Autor

En la Tabla 26 se presenta la cantidad de registros por fecha durante un periodo de 4 meses, en el cual se evidencia una notable disminución en los eventos registrados.

Tabla 26 Registros de eventos antispam/antivirus por meses
Fuente: Autor

Fecha	Cantidad
16 noviembre 2023	77.446
17 noviembre 2023	50.824
13 diciembre 2023	4.008
3 enero 2024	2.717
10 enero 2024	1.386
16 enero 2024	2.531
6 febrero 2024	1.22
23 febrero 2024	9.931

4.3 Pentesting

Para verificar el estado actual del servicio de comunicación asíncrona y garantizar la vigencia de sus medidas de seguridad, se realiza una prueba de estrés pentesting. Esta prueba se lleva a cabo desde una máquina virtual que ejecuta el sistema operativo Kali Linux, una herramienta esencial en el ámbito del pentesting, especialmente en entornos donde se busca identificar y mitigar vulnerabilidades de seguridad. En el presente estudio, Kali Linux se utiliza como plataforma principal para realizar pruebas de penetración y evaluar la efectividad de las medidas de mitigación implementadas.

A continuación, se utiliza la herramienta NMAP, integrada en Kali Linux, para llevar a cabo un análisis de la IP directa del servicio de comunicación asíncrona. La Figura 37 muestra el proceso de ataque con sploits, el cual proporciona información básica sobre el servicio, como los puertos detectados y su estado. Además, permite identificar qué puertos están abiertos y qué servicios se están ejecutando en ellos. Esta información es crucial para evaluar la vulnerabilidad del sistema y determinar posibles puntos de ataque.

```
└─$ nmap 192.68.0.92 --script smtp-enum-users.nse
Starting Nmap 7.92 ( https://nmap.org ) at 2024-02-19 11:51 EST
Nmap scan report for 192.68.0.92
Host is up (0.66s latency).
Not shown: 901 filtered tcp ports (no-response), 72 filtered tcp ports (host-unreach)
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   closed ssh
25/tcp   open   smtp
| smtp-enum-users:
|_
53/tcp   closed domain
80/tcp   open   http
110/tcp  open   pop3
139/tcp  closed netbios-ssn
143/tcp  open   imap
389/tcp  open   ldap
443/tcp  open   https
445/tcp  closed microsoft-ds
465/tcp  open   smtps
| smtp-enum-users:
|   Method RCPT returned a unhandled status code.
|_  Method VRFY returned a unhandled status code.
587/tcp  open   submission
| smtp-enum-users:
|   Method RCPT returned a unhandled status code.
|_  Method VRFY returned a unhandled status code.
636/tcp  closed ldapssl
993/tcp  open   imaps
995/tcp  open   pop3s
2222/tcp closed EtherNetIP-1
3128/tcp closed squid-http
5901/tcp closed vnc-1
6001/tcp closed X11:1
7025/tcp open   vmsvc-2
8080/tcp closed http-proxy
8443/tcp open   https-alt
9071/tcp closed unknown
10000/tcp open  snet-sensor-mgmt
10024/tcp closed unknown
10025/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 70.15 seconds
```

Figura 36 Primer ataque con sploits al servicio de comunicación asíncrona. Fuente: Autor

En el segundo intento de ataque al servicio de comunicación asíncrona con sploits, se selecciona el sploit "smtp", el cual emplea una técnica de fuerza bruta para intentar acceder al servidor a través del puerto 25. Los ataques de fuerza bruta son métodos comúnmente utilizados

por los atacantes para intentar descifrar contraseñas y acceder a cuentas de usuario sin autorización (Urtiaga, 2023).

Este ataque es detectado rápidamente por el firewall, que actúa de manera inmediata al colocar la dirección IP del atacante en una lista negra de conexiones. Esto se puede observar en la Figura 38, donde se registra la acción del firewall para bloquear la conexión entrante desde la dirección IP del atacante.

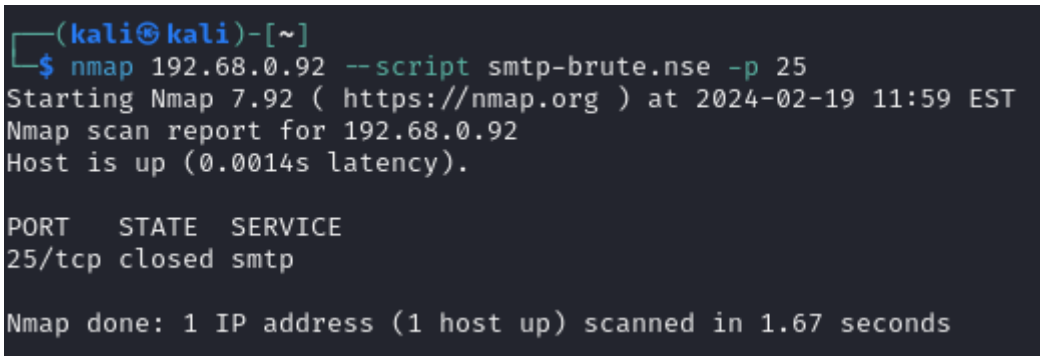


Figura 37 Segundo ataque al servicio de comunicación asíncrona con sploits. Fuente: Autor

En la Figura 39, se identifica la dirección IP de la máquina atacante.

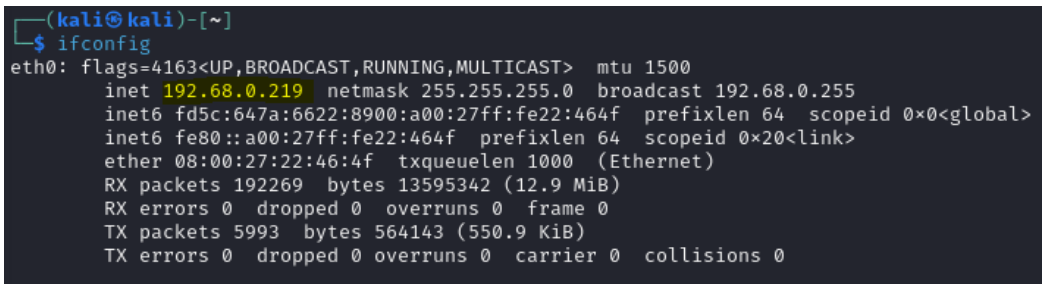


Figura 38 Dirección IP de la maquina atacante. Fuente: Autor

A continuación, en la Figura 40, se verifica desde el servidor que la dirección IP del atacante ha sido bloqueada por la herramienta Fail2ban, configurada en el servidor.

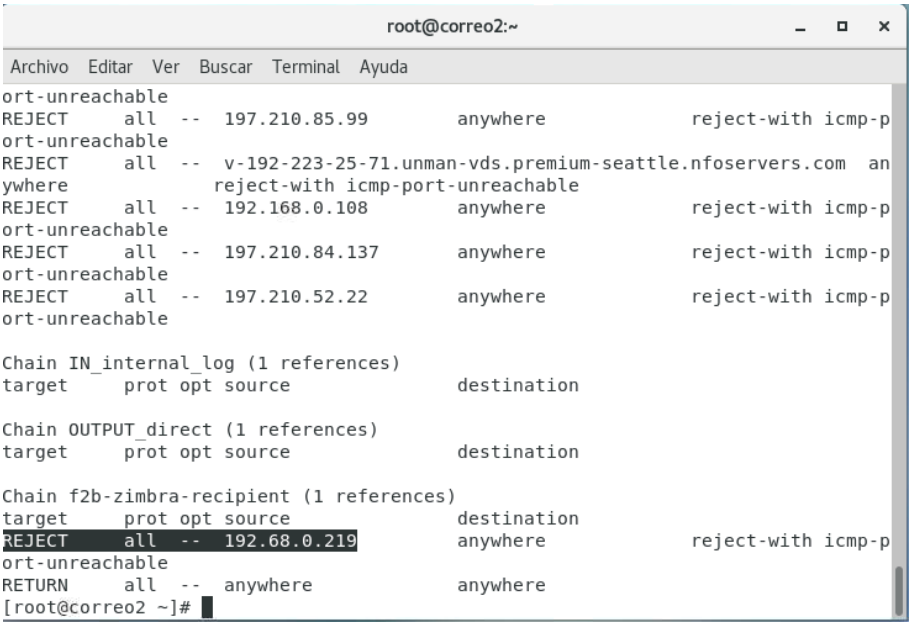


Figura 39 Bloqueo de IP atacante desde el servido. Fuente: Autor

La siguiente prueba de estrés a la que se somete al servidor es con la herramienta Metasploit, usando dentro de Kali Linux. En la Figura 41 se muestra la información sobre el dominio y el servicio que se está ejecutando en la dirección IP donde está alojado el servidor. De igual manera, no se permite obtener más que información básica, dado que la configuración de seguridad está aplicada.

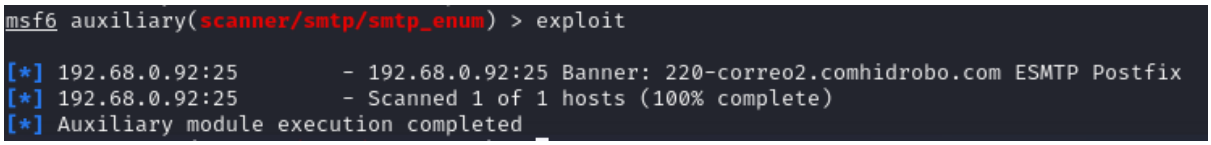


Figura 40 Ataque con Metasploit. Fuente: Autor

Los hallazgos de este estudio muestran una alineación clara con los objetivos específicos del proyecto. Inicialmente, se realizó un diagnóstico exhaustivo del servicio de comunicación asíncrona de la institución mediante escaneos especializados, lo que permitió una identificación precisa de las vulnerabilidades existentes, cumpliendo así con el primer objetivo. Posteriormente, se implementaron los controles CIS Controls v.8 adecuados al servidor de comunicación asíncrona, integrando de manera efectiva tanto la Norma ISO/IEC 27001:2022 como la metodología MAGERIT v. 3, lo que contribuyó significativamente a mitigar las vulnerabilidades, conforme al segundo objetivo. Finalmente, se realizó una evaluación completa del nivel de mejora del servicio de comunicación asíncrona de la empresa Comercial Hidrobo S.A., proporcionando una visión integral de los avances realizados, lo que confirma

el cumplimiento del tercer objetivo del proyecto. En conjunto, estos resultados respaldan la efectividad y el éxito del estudio en la consecución de los objetivos propuestos.

CAPITULO V

CONCLUSIONES

La implementación de los controles CIS v.8 ha demostrado una mejora significativa en la seguridad de la información en Comercial Hidrobo S.A., reduciendo eficazmente los riesgos de brechas de seguridad, pérdida de datos y ataques cibernéticos, lo que garantiza la integridad, disponibilidad y confidencialidad de la información crítica y sensible.

La metodología MAGERIT v.3 ha proporcionado un enfoque estructurado y sistemático para evaluar y gestionar los riesgos de seguridad de la información en la empresa. Al integrarse con los controles CIS v.8 y las directrices de la norma ISO/IEC 27001:2022, Comercial Hidrobo S.A. ha logrado identificar con mayor precisión las vulnerabilidades en su sistema de comunicación asíncrona y aplicar medidas correctivas para mitigarlas.

La incorporación de la Norma ISO/IEC 27001:2022 junto con la implementación de los controles CIS v.8 asegura el cumplimiento de estándares internacionales en seguridad de la información por parte de Comercial Hidrobo S.A., lo que refuerza su compromiso con la protección de datos y el cumplimiento de la normativa vigente ante clientes, proveedores y reguladores.

La integración de estas tres herramientas ha mejorado no solo el servicio de comunicación asíncrona al que se aplicaron, sino que también ha fortalecido la posición de Comercial Hidrobo S.A. frente a posibles amenazas cibernéticas presentes y futuras. Esta implementación no solo protege los activos digitales de la empresa, sino que también salvaguarda su reputación, la confianza del cliente y la continuidad operativa en un entorno empresarial cada vez más digitalizado y peligroso.

RECOMENDACIONES

Se sugiere llevar a cabo una campaña continua de concientización y sensibilización entre los colaboradores de Comercial Hidrobo S.A., dado que diariamente surgen nuevas vulnerabilidades de seguridad que pueden ser aprovechadas por ciberdelincuentes.

Es recomendable implementar un programa de capacitación completo para promover el uso adecuado de la información en el servicio de comunicación asíncrona, priorizando la confidencialidad, integridad y disponibilidad de los datos.

Se aconseja realizar una evaluación continua de las amenazas y riesgos, ya que la tecnología evoluciona rápidamente y es fundamental estar al tanto de los cambios para poder reaccionar de manera efectiva y prevenir posibles ataques al servicio de comunicación asíncrona.

Se recomienda establecer un registro de eventos (bitácora) para documentar cómo se abordan y resuelven los ataques que puedan surgir, lo que permitirá una respuesta más ágil y eficiente ante futuros incidentes.

REFERENCIAS

Acosta Nexar, C. F. (02 de 2018). *REPOSITORIO UNIVERSIDAD LAICA "ELOY ALFARO" DE MANABI.* Obtenido de https://repositorio.uleam.edu.ec/bitstream/123456789/2668/1/ULEAM-INFOR-0084.pdf

Altamirano-de-la-Borda, K. J. (2020). La seguridad de la información . *III Congreso Internacional de Ingeniería de Sistemas*, 19.

Américo Estrada, E. A. (2022). *Cómoelaborar tu Tesisde Gradoy no morir en el intento.* Cuzco.

Arias, F. (2016). *El proyecto e investigación.* Caracas: Edisiones el Pasillo.

CABEZAS, S. (25 de 11 de 2022). *REPOSITORIO PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR.*

Digital, T. (17 de 6 de 2020). Obtenido de https://tecpro-digital.com/plantillas-de-diagramas-de-ishikawa-en-word/

Ecuador, R. d. (2021). *Registro oficial.* Quito.

España, G. d. (10 de 2012). *Portal de Administración Eletrónica.* Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XFSfLlVKiUk

Fyodor. (2023). *NMAP:ORG*. Obtenido de https://nmap.org/man/es/index.html

g0tmi1k. (03 de Noviembre de 2004). *Kali Linux org*. Obtenido de Documentación: https://www.kali.org/docs/introduction/what-is-kali-linux/

Gomez, Á. (2014). *Enciclopedia de la Seguridad Informática.* Madrid: RA-MA, S.A. Editorial y Publicaciones.

González, P. (28 de 02 de 2023). *Sello Legal*. Obtenido de https://sellolegal.com/blog/los-casos-de-phishing-mas-sonados-de-la-historia-de-internet/

Guaman, V. (08 de 07 de 2019). *Repositorio Universidad Tecnica del Norte.* Obtenido de Repositorio Universidad Tecnica del Norte: https://repositorio.utn.edu.ec/bitstream/123456789/9535/2/04%20ISC%20524%20TRABAJO%20DE%20GRADO.pdf

Hernández, C. (11 de 07 de 2019). *Respositorio Universidad Tecnia del Norte.* Obtenido de https://repositorio.utn.edu.ec/bitstream/123456789/9534/2/04%20ISC%20523%20TRABAJO%20GRADO.pdf

Honores, L. (09 de 2021). *Repositorio de la Escuela Politecnica Superioir de Chimborazo.* Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/14702/1/20T01447.pdf

ISO, O. (2022). Obtenido de https://www.iso.org/standard/27001

Javier Guaña, A. S. (16 de 08 de 2022). *Proquest.* Obtenido de https://www.proquest.com/openview/02492b51bc001f7bf3254a198698d1d7/1?pq-origsite=gscholar&cbl=1006393

Juan A. Figueroa-Suárez, R. F.-A.-O.-G. (2017). La seguridad informática y la seguridad de la información. *Polo del Conocimiento,* 11.

Kaspersky, L. (2023). *Kaspersky Lab*. Obtenido de Kaspersky Lab.

ONU. (2023). *ONU*. Obtenido de https://ecuador.un.org/es

OpenVas. (31 de 05 de 2023). *OpenVas*. Obtenido de https://openvas.org/

Quirola, L. (08 de 2019). *Respositorio Universidad Tecnica de Ambato.*

Ramos, J. (2022). *Como protegerte del phishing.* Berlin: Verlag GD Publishing Ltd.& Co KG.

Sanchez, E. (2018). *PLAN DE CONTINGENCIA INFORMÁTICO.* Ibarra.

Sanchez, E. (2020). *Intranet.* Obtenido de http://capacita.comhidrobo.com/docu/sistemas/politica/#p=1

Security, C. f. (05 de 2021). *CIS Critical Security Controls*. Obtenido de https://www.cisecurity.org/controls

Technology, N. I. (s.f.). *National Institute of Standards and Technology*. Obtenido de https://nvd.nist.gov/vuln-metrics/cvss

Tenable. (15 de 11 de 2018). *Tenable Plugins*. Obtenido de https://www.tenable.com/plugins/nessus/52633

Tenable. (26 de 06 de 2019). *Tenable*. Obtenido de https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/datasheets/NessusP

Urtiaga, G. G. (21 de 01 de 2023). *Google Libros.* Obtenido de Google Libros: https://www.google.com.ec/books/edition/Gu%C3%ADa_de_seguridad_en_WordPress/iaWoEAAAQBAJ?hl=es&gbpv=1&dq=ataque+de+fuerza+bruta&pg=PA55&printsec=frontcover

UTN. (2016). *Lineas de Investigación*. Obtenido de https://software.utn.edu.ec/investigacion/lineas-de-investigacion/

ANEXOS

Anexo 1: Acuerdo de confidencialidad para el desarrollo del proyecto de tesis en la empresa Comercial Hidrobo S.A

COMERCIAL HIDROBO
¡Decisión Inteligente!

ACUERDO DE CONFIDENCIALIDAD

Comparece, por una parte, la empresa COMERCIAL HIDROBO S.A. COMHIDROBO (en adelante LA EMPRESA), con RUC No. 1090084247001, debidamente representada por el señor Hidrobo Estrada Ángel Patricio en su calidad de Gerente General, y como tal Representante Legal, a quien para efectos del presente acuerdo se le denominará en adelante como "LA EMPRESA"; y, por otra parte, comparece la señorita MAFLA FLORES SAMANTHA MONSERRAT, por sus propios y personales derechos en calidad de tesista de LA EMPRESA, a quién en adelante y para efectos del presente instrumento se lo denominará "TESISTA", quien en forma libre y voluntaria y por los derechos que representa, conviene en suscribir el presente Acuerdo de Confidencialidad.

CLAUSULA PRIMERA: OBJETO. - El objeto de este acuerdo es la protección de la Información que maneja EL TESISTA respecto de LA EMPRESA, información en que LA EMPRESA figura como titular, responsable o encargado del tratamiento de datos personales de conformidad con la Ley Orgánica de Protección de Datos Personales.

CLAUSULA SEGUNDA: DEFINICIONES. -

A efectos del presente acuerdo, se tendrá en cuenta las siguientes definiciones:

2.1 Conocimientos o información pública: Se trata de toda aquella información que es de dominio público y que forma parte de la propia profesión, especialización o conocimiento de EL TESISTA.

2.2 Conocimientos técnicos: Aquellos conocimientos que se refieren al giro del negocio o aspectos técnicos de LA EMPRESA que tienen un contenido valioso por referirse a operaciones o gestión de negocio.

Para que los conocimientos técnicos deban ser manejados con el carácter de confidenciales, no será necesario que LA EMPRESA manifieste expresamente su voluntad de que no sean comunicados a terceros, por lo que deben mantenerse con carácter confidencial; por ello EL TESISTA debe advertir que la divulgación de los conocimientos a los que tiene acceso ocasionará un daño a LA EMPRESA, a sus clientes o a terceros.

2.3 Información no divulgada o confidencial: Toda información relacionada con las que se enuncia sin que la enumeración sea restrictiva: información estratégica, jurídica, financiera, de mercadeo, información y proyecciones de planes de negocios, datos, registros de negocios, lista de clientes y proveedores, contratos con proveedores, planes de venta y mercadeo, lista de empleados, políticas y procedimientos, información relacionada con los procesos, técnicas, tecnologías, programas de software, códigos de fuente, esquemas, diseños o teorías y en general toda información que se refiera a la "relación", negocios y actividades que realice LA EMPRESA especialmente a sus activos, ubicación de los mismos, costos, estados, etc. También se considerará confidencial tota información que mantenga LA EMPRESA respecto de sus clientes o cualquier información relacionada con su trabajo directo, incluyendo información personal que ha tratado LA EMPRESA de titulares, responsables, encargados o de terceros, de conformidad con la Ley Orgánica de Protección de Datos Personales.

La información confidencial incluirá toda información que sea secreta o personal que tenga la protección determinada en la ley, tenga un valor comercial efectivo o potencial y se haya adoptado medidas razonables para mantenerla secreta.

COMERCIAL HIDROBO
¡Decisión Inteligente!

2.4 Competencia desleal: Todo hecho, acto o práctica contrario a los usos o costumbres honestas en el desarrollo de actividades económicas, en especial la divulgación, adquisición o uso de información sin el consentimiento de LA EMPRESA, al igual que la prestación de servicios o venta de productos a clientes de manera directa, a través de la creación de una relación entre EL TESISTA y terceras personas.

2.5 Riesgo de divulgación y competencia desleal: El acceso por parte de EL TESISTA a la información mencionada en los numerales 2.2, 2.3 y 2.4, abre la posibilidad de que dicha información sea divulgada a terceros, como por ejemplo otras empresas o personas naturales que compitan con las actividades de LA EMPRESA, o que sea utilizada por EL TESISTA directamente o a través de terceros, ya sea actuando por su propia cuenta o al servicio de empresas competidoras.

CLAUSULA TERCERA: OBLIGACIONES DEL TESISTA. - EL TESISTA declara, acepta y se obliga a lo siguiente:

a) Toda Información entregada por LA EMPRESA o a la que haya tenido acceso EL TESISTA, de aquella referida en los puntos 2.2. y 2.3 del presente documento, sea escrita, tangible o electrónica, se considerará confidencial. La Información provista al TESISTA de manera visual u oral debe estar designada por LA EMPRESA como confidencial en el momento en que se la revela.

b) EL TESISTA no revelará la Información Confidencial de LA EMPRESA (descrita como tal en los puntos 2.2. y 2.3 del presente documento), a ninguna persona, con excepción de aquellas personas que: i) por su posición o cargo necesariamente requieran conocerla, mi) han sido informados sobre la confidencialidad de dicha Información, y, iii) cuente con autorización expresa y por escrito de la Parte que revela dicha Información Confidencial. EL TESISTA antes de revelar la Información Confidencial a las mencionadas personas, deberá informarlas de la naturaleza reservada de la misma;

c) EL TESISTA tratará la Información Confidencial (descrita como tal en los puntos 2.2. y 2.3 del presente documento) con el mismo cuidado y discreción que tiene con su propia información confidencial, que en todo caso no será menor que un estándar razonable de cuidado, de modo que se evite que dicha Información sea relevada, publicada o diseminada. Consecuentemente, E EL TESISTA deberá hacer que todas las personas que hayan tenido acceso a la Información Confidencial mantengan estricta reserva sobre la misma. La violación del presente convenio por parte de las personas mencionadas se considerará como violación del EMPLEADO a este acuerdo.

d) LA EMPRESA podrá revelar la Información Confidencial a EL TESISTA de manera oral, visual, escrita, electrónica, magnética o por cualquier otra forma, únicamente para cumplir el objeto del contrato que se suscribirá entre las mismas o para beneficio comprobado de la parte que revela la Información Confidencial;

e) EL TESISTA podrá hacer copias, notas, resúmenes, o abstractos de Información ya sea de manera tangible o electrónica, solamente según sea necesario para el uso que se autoriza en el presente Acuerdo. Todas las copias, notas, resúmenes, o abstractos de Información ya sean en forma tangible o electrónica, podrán ser utilizadas o analizadas para efectos del cumplimiento estricto de sus funciones dentro del contrato de trabajo que tiene suscrito con LA EMPRESA.

COMERCIAL HIDROBO
¡Decisión Inteligente!

f) Cuando EL TESISTA conozca de cualquier pérdida, uso no autorizado o revelación de la Información Confidencial de LA EMPRESA o que ésta trate, EL TESISTA deberá comunicar inmediatamente por escrito a LA EMPRESA de tal pérdida, uso no autorizado o revelación. EL EMPLEADO acuerda tomar los pasos necesarios para ayudar a LA EMPRESA a remediar tal uso no autorizado o revelación de la Información Confidencial.

g) Se deja constancia que EL TESISTA deberá cumplir las obligaciones de no divulgación en los términos del presente acuerdo, aun cuando las partes por cualquier motivo hayan decidido no continuar su relación laboral y/o el acuerdo a ser suscrito.

h) EL TESISTA, mientras se encuentre en relación de dependencia, se compromete a no efectuar competencia o desarrollar actividades que por sí mismo o por cuenta de terceros, gire en el mismo ámbito de negocio que LA EMPRESA.

CLÁUSULA CUARTA: OBLIGACIÓN DE LAS PARTES. -

a) Las Partes en su condición responsables directos e indirectos del tratamiento de datos personales, se comprometen a respetar en todo momento la normativa vigente en materia de protección de datos de carácter personal y lo establecido en este documento.

b) Las Partes, tratarán los datos personales a los que tengan acceso, única y exclusivamente para el desarrollo y gestión de sus actividades conforme a lo establecido en el presente Contrato, obligándose a:

(i)

No aplicar, ni utilizar, ni revelar dichos datos de carácter personal con fines distintos a los que se derivan de su actividad conforme a lo establecido en el presente Contrato.

(ii)

No comunicar, ni permitir el acceso a los datos de carácter personal a ningún tercero.

(iii) Las Partes, se comprometen a adoptar, actualizar y mantener las medidas organizativas y técnicas que estime necesarias para garantizar la seguridad y confidencialidad de los datos de carácter personal, impidiendo cualquier alteración, perdida, tratamiento, procesamiento o acceso no autorizado. Esta obligación se desarrollará de conformidad con el estado de la tecnología, la naturaleza de los datos y los riesgos a los que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

CLAUSULA QUINTA; EXCEPCIONES. - Las obligaciones arriba descritas no serán aplicables cuando EL TESISTA demuestre que:

a) La Información de LA EMPRESA al momento de la revelación se volvió parte del dominio público conforme lo mencionado en el numeral 2.1 del presente acuerdo, mediante una publicación o cualquier otro medio distinto, siempre que dicha publicación no sea imputable a EL TESISTA;

COMERCIAL HIDROBO
¡Decisión Inteligente!

b) La Información Confidencial haya sido requerida por autoridad competente y de acuerdo a la ley.

CLAUSULA SEXTA: LIMITACIONES A LA INFORMACIÓN CONFIDENCIAL PROPORCIONADA POR LA EMPRESA. - EL TESISTA no identificará a LA EMPRESA, o a cualquier otro dueño de la Información, en cualquiera de los siguientes medios: propaganda publicitaria, material de venta, boletín de prensa, revelación pública, o de manera pública, sin la previa autorización dada por escrito por LA EMPRESA.

Ninguna licencia bajo cualquier marca registrada, patente, derechos de propiedad literaria, secretos comerciales, u otros derechos de propiedad intelectual se entienden dados, otorgados o implicados cuando se revela información al TESISTA.

CLAUSULA SÉPTIMA: PLAZO DE CONFIDENCIALIDAD. - Por la naturaleza de este acuerdo, el secreto y confidencialidad de la información conocida o proporcionada por LA EMPRESA al TESISTA, se mantendrá de forma indefinida. Este acuerdo solo dejará de regir LA EMPRESA desclasifique su información confidencial o que dicha información con el tiempo se circunscriba en lo dispuesto en el numeral 2.1

Ante la terminación de este Acuerdo, EL TESISTA cesará inmediatamente el uso de la Información Confidencial y la devolverá inmediatamente a LA EMPRESA, sin realizar ningún tipo de copia o registro.

CLAUSULA OCTAVA: DISPOSICIONES GENERALES. -

a) Este Acuerdo no obliga a LA EMPRESA a revelar Información Confidencial.

b) EL TESISTA no podrá ceder sus derechos ni delegar sus obligaciones o responsabilidades sin el consentimiento previo y por escrito de LA EMPRESA.

c) El presente acuerdo solo podrá ser modificado por mutuo acuerdo y por escrito.

d) Las comunicaciones y notificaciones que deban hacer serán entregadas personalmente en sus oficinas.

e) Ningún término o disposición contenida se considerará renuncia por LA EMPRESA, salvo que esa renuncia o consentimiento sea por escrito y firmado por LA EMPRESA.

f) EL TESISTA y LA EMPRESA notificarán por escrito, mutuamente, los nombres de las partes autorizadas, para recibir o dar la Información Confidencial, así como el detalle de la información que sea requerida. EL TESISTA será responsable de la buena utilización que hagan sus funcionarios autorizados de la información entregada por LA EMPRESA.

g) Invalidez Parcial: Cuando una o varias disposiciones de este Acuerdo se declaren nulas, ineficaces o contrarias a la ley, ello no implicará la nulidad, ineficacia o ilegalidad de las disposiciones restantes, que seguirán siendo vinculantes y obligatorias para las partes y permanecerán en pleno vigor.

h) Convenio Total: Este Convenio contiene los términos y condiciones que regirán el manejo de la información confidencial a la que tenga acceso EL EMPLEADO, y tiene prioridad sobre cualquier convenio verbal o escrito existente entre las partes.

COMERCIAL HIDROBO
¡Decisión Inteligente!

CLÁUSULA NOVENA: RESPONSABILIDAD EN CASO DE INCUMPLIMIENTO:

En caso de que EL TESISTA incumpla las obligaciones que asume a través del presente acuerdo, deberá pagar a LA EMPRESA la indemnización por daños que el incumplimiento de este contrato le haya producido, incluyendo el derecho de repetición por las indemnizaciones que terceros sigan a LA EMPRESA por el incumplimiento a la confidencialidad determinada en el presente acuerdo.

Adicionalmente, LA EMPRESA podrá iniciar otras las acciones que le permitan la ley, inclusive aquellas e índole penal.

CLÁUSULA DÉCIMA: RESOLUCIÓN DE CONTROVERSIAS. - Toda controversia que no puedan solucionarse de mutuo acuerdo se someterá a la resolución de un Tribunal de Arbitraje administrado por la Cámara de Comercio de Ibarra, de acuerdo con la Ley de Arbitraje y Mediación y Reglamento del Centro de Arbitraje de dicha Cámara, y las siguientes normas:

a) Los árbitros serán seleccionados conforme a lo establecido en la Ley de Arbitraje y Mediación Ecuatoriana. El Tribunal Arbitral estará conformado por tres árbitros. Las partes elegirán de común acuerdo a dos árbitros de la Lista del Centro de Arbitraje y Mediación de la Cámara de Comercio de Ibarra. De no existir acuerdo entre las partes, los dos árbitros se elegirán por sorteo realizado por el Centro. Los dos árbitros seleccionados, ya sea por acuerdo o por sorteo, elegirán al tercero;

b) Las partes renuncian a la jurisdicción ordinaria, se obligan a acatar el laudo que expida el Tribunal Arbitral y se comprometen a no interponer ningún tipo de recurso en contra del laudo dictado, a más de los permitidos por la ley;

c) El procedimiento será confidencial;

d) El Tribunal fallará en derecho;

e) Para la ejecución de medidas cautelares, el Tribunal Arbitral está facultado para solicitar de los funcionarios públicos, judiciales, policiales y administrativos su cumplimiento, sin que sea necesario recurrir a juez ordinario alguno;

f) El lugar del arbitraje será las instalaciones del Centro de Arbitraje y Mediación de la Cámara de Comercio de Ibarra;

g) Las acciones de naturaleza penal se resolverán de conformidad con el Código Penal.

En señal de constancia y fiel cumplimiento, la parte suscribe el Acuerdo de Confidencialidad, en dos ejemplares de un mismo tenor, en esta ciudad de Ibarra, a los 25 días del mes de julio del año 2023.

TESISTA

Samanta Mafla Flores
C.I. 1003637061

LA EMPRESA

Patricio Hidrobo Estrada
RUC: 1090084247001

Anexo 2: Reporte del Análisis de vulnerabilidades de Nessus Essentials

correo.comhidrobo.com

0	1	17	0	173
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Sep 13 13:31:22 2023
End time: Wed Sep 13 14:06:37 2023

Host Information

DNS Name: correo.comhidrobo.com
IP: 190.110.206.46
OS: AIX 5.3

Vulnerabilidades

42873 - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

31705 - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers.

Description

The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack.

Note: This is considerably easier to exploit if the attacker is on the same physical network.

See Also

http://www.nessus.org/u?3a040ada

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers.

51192 - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted.

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below:

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

See Also

https://www.itu.int/rec/T-REC-X.509/en

https://en.wikipedia.org/wiki/X.509

Solution

Purchase or generate a proper SSL certificate for this service.

15901 - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired.

Description

This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired.

Solution

Purchase or generate a new SSL certificate to replace the existing one.

65821 - SSL RC4 Cipher Suites

Synopsis

The remote service supports the use of the RC4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness.

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext.

See Also

https://www.rc4nomore.com/

http://www.nessus.org/u?ac732a0

http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/

https://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

Solution

Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

57582 - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

Description

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority.

Solution

Purchase or generate a proper SSL certificate for this service.

52633 - Unprotected memcached

Synopsis

Memcached is running on a public IP address.

Description

Memcached is a memory-based object store. As it is designed for performance, this program does not contain any security mechanism (ie: authentication), meaning that anyone can connect to this server and perform queries against it.

See Also

http://memcached.org/

http://web.archive.org/web/20100710073600/http://www.eu.socialtext.net:80/memcached/index.cgi?

https://www.mediawiki.org/wiki/Memcached

Solution

Make sure that the machine is properly protected by a firewall and that traffic to the port is restricted to authorized hosts.

Anexo 3: Check list aplicación de controles CIS v.8 en Comercial Hidrobo S.A.

CHECK LIST APLICACIÓN DE CIS CONTROLS v8 en COMERCIAL HIDROBO S.A.							
CIS Control	CIS Salvaguarda	Tipo de Activo	Función de seguridad	Título	Descripción	Nov 2023	Enero 2024
1				Inventario y Control de Activos Empresariales			
				Gestionar activamente (inventariar, rastrear y corregir) todos los activos empresariales (Dispositivos de usuario final, incluidos dispositivos portátiles y móviles; Dispositivos de red; Dispositivos no informáticos/Internet de las cosas (IoT); y servidores) conectados a la infraestructura física, virtualmente, de forma remota y aquellos dentro de entornos de nube, para conocer con precisión la totalidad de los activos que deben monitorearse y Protegerse dentro de la empresa. Esto también respaldará la identificación de activos no autorizados y no administrados para eliminarlos o remediarlos. Administre activamente (inventario, seguimiento y corrección) todos los activos empresariales (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/Internet de las cosas (IoT); y servidores) conectados a la infraestructura física, virtualmente, de forma remota y aquellos dentro de entornos de nube, para conocer con precisión la totalidad de los activos que deben monitorearse y Protegerse dentro de la empresa. Esto también ayudará a identificar activos no autorizados y no administrados para eliminarlos o remediarlos.		
1	1.1	Dispositivos	Identificar	Establecer y mantener un inventario detallado de activos empresariales	Establecer y mantener un inventario preciso, detallado y actualizado de todos los activos empresariales con potencial para almacenar o procesar datos, que incluya: Dispositivos de usuario final (incluidos portátiles y móviles), Dispositivos de red, no Informáticos/IoT, Dispositivos y servidores. Asegúrese de que el Inventario registre la dirección de red (si es estática), la dirección de hardware, el nombre de la máquina, el propietario de los activos empresariales, el departamento de cada activo y si el activo ha sido aprobado para conectarse a la red. Para Dispositivos de usuarios finales móviles, las herramientas de tipo MDM pueden respaldar este proceso, cuando corResponderá. Este inventario incluye activos conectados a la infraestructura de forma física, virtual, remota y aquellos dentro de entornos de nube. Además, incluye activos que están conectados periódicamente a la infraestructura de red de la empresa, incluso si no están bajo el control de la empresa. Revise y actualice el inventario de todos los activos de la empresa cada dos años o con mayor frecuencia.	x	x
1	1.2	Dispositivos	Responder	Abordar activos no autorizados	Asegúrese de que exista un proceso para abordar los activos no autorizados semanalmente. La empresa puede optar por eliminar el activo de la red, negarle la conexión remota a la red o ponerlo en cuarentena.		x
1	1.3	Dispositivos	Detectar	Utilice una herramienta de descubrimiento activo	Utilice una herramienta de descubrimiento activo para identificar activos conectados a la red de la empresa. Configure la herramienta de descubrimiento activo para que se ejecute diariamente o con mayor frecuencia.		x
1	1.4	Dispositivos	Identificar	Utilice el registro del Protocolo de configuración dinámica de host (DHCP) para actualizar el inventario de activos empresariales	Utilice el registro DHCP en todos los servidores DHCP o herramientas de administración de direcciones de Protocolo de Internet (IP) para actualizar el inventario de activos de la empresa. Revise y utilice registros para actualizar el inventario de activos de la empresa semanalmente o con mayor frecuencia.		x
1	1.5	Dispositivos	Detectar	Utilice una herramienta de descubrimiento pasivo de activos	Utilice una herramienta de descubrimiento pasivo para identificar activos conectados a la red de la empresa. Revise y utilice escaneos para actualizar el inventario de activos de la empresa al menos semanalmente o con mayor frecuencia.		X
2				Inventario y Control de Activos de Software			
				Administre activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y pueda ejecutar software autorizado, y que se encuentre software no autorizado y no administrado y se impida su instalación o ejecución. Administre activamente (inventario, seguimiento y corrección) todo el software (sistemas operativos y aplicaciones) en la red para que solo se instale y pueda ejecutar software autorizado, y que se encuentre software no autorizado y no administrado y se impida su instalación o ejecución.		
2	2.1	Aplicaciones	Identificar	Establecer y mantener un inventario de software	Establezca y mantenga un inventario detallado de todo el software con licencia instalado en los activos empresariales. El inventario de software debe documentar el título, el editor, la fecha de instalación/uso inicial y el propósito comercial de cada entrada; cuando corresponda, incluya el localizador uniforme de recursos (URL), las tiendas de aplicaciones, las versiones, el mecanismo de implementación y la fecha de desmantelamiento. Revise y actualice el inventario de software cada dos años o con mayor frecuencia.		X
2	2.2	Aplicaciones	Identificar	Asegúrese de que el software autorizado sea actualmente compatible	Asegúrese de que solo el software actualmente admitido esté designado como autorizado en el inventario de software para activos empresariales. Si el software no tiene soporte, pero es necesario para el cumplimiento de la misión de la empresa, documente una excepción que detalle los controles de mitigación y la aceptación del riesgo residual. Para cualquier software no compatible sin documentación de excepción, designe como no autorizado. Revise la lista de software para verificar el soporte del software al menos una vez al mes o con mayor frecuencia.	X	X
2	2.3	Aplicaciones	Responder	Abordar el software no autorizado	Asegúrese de que el software no autorizado se elimine del uso en los activos empresariales o reciba una excepción documentada. Revise mensualmente o con mayor frecuencia.		X
2	2.4	Aplicaciones	Detectar	Utilice herramientas de inventario de software automatizadas	Utilice herramientas de inventario de software, cuando sea posible, en toda la empresa para automatizar el descubrimiento y la documentación del software instalado.		X
2	2.5	Aplicaciones	Proteger	Software autorizado en la lista de permitidos	Utilice controles técnicos, como listas de aplicaciones permitidas, para garantizar que solo se pueda ejecutar o acceder al software autorizado. Reevaluar cada dos años o con mayor frecuencia.	X	X
2	2.6	Aplicaciones	Proteger	Lista de bibliotecas autorizadas permitidas	Utilice controles técnicos para garantizar que solo las bibliotecas de software autorizadas, como archivos específicos .dll, .ocx, .so, etc., puedan cargarse en un proceso del sistema. Bloquee la carga de bibliotecas no autorizadas en un proceso del sistema. Reevaluar cada dos años o con mayor frecuencia.	X	X
2	2.7	Aplicaciones	Proteger	Lista de scripts autorizados permitidos	Utilice controles técnicos, como firmas digitales y control de versiones, para garantizar que solo se permitan ejecutar scripts autorizados, como archivos .ps1, .py, etc. específicos. Bloquea la ejecución de scripts no autorizados. Reevaluar cada dos años o con mayor frecuencia.		X
3				Protección de datos			
				Desarrollar procesos y controles técnicos para identificar, clasificar, manejar, retener y disponer de forma segura los Datos.			
3	3.1	Datos	Identificar	Establecer y mantener un proceso de gestión de datos	Establecer y mantener un proceso de gestión de datos. En el proceso, aborde la sensibilidad de los datos, el propietario de los datos, el manejo de los datos, los límites de retención de datos y los requisitos de eliminación, según los estándares de sensibilidad y retención de la empresa. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar esta Salvaguarda.		X
3	3.2	Datos	Identificar	Establecer y mantener un inventario de datos	Establecer y mantener un inventario de Datos, basado en el proceso de gestión de Datos de la empresa. Datos sensibles al inventario, como mínimo. Revisar y actualizar el inventario anualmente, como mínimo, con prioridad en Datos sensibles.		X
3	3.3	Datos	Proteger	Configurar listas de control de acceso a datos	Configure listas de control de acceso a Datos según la necesidad de conocimiento del usuario. Aplicar listas de control de acceso a Datos, también conocidas como permisos de acceso, a sistemas de archivos locales y remotos, Bases de Datos y Aplicaciones.		X
3	3.4	Datos	Proteger	Hacer cumplir la retención de datos	Conservar los Datos de acuerdo con el proceso de gestión de Datos de la empresa. La retención de datos debe incluir plazos mínimos y máximos.	X	X
3	3.5	Datos	Proteger	Eliminar datos de forma segura	Disponer de forma segura de los Datos como se describe en el proceso de gestión de Datos de la empresa. Asegúrese de que el proceso y el método de eliminación sean acordes con la sensibilidad de los Datos.	X	X

3	3.6	Dispositivos	Proteger	Cifrar datos en dispositivos de usuario final	Cifrar Datos en Dispositivos de usuario final que contengan Datos confidenciales. Las implementaciones de ejemplo pueden incluir: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.		X
3	3.7	Datos	Identificar	Establecer y mantener un esquema de clasificación de datos	Establecer y mantener un esquema general de clasificación de Datos para la empresa. Las empresas pueden utilizar etiquetas, como "Sensible", "Confidencial" y "Público", y clasificar sus Datos de acuerdo con esas etiquetas. Revisar y actualizar el esquema de clasificación anualmente, o cuando ocurran cambios empresariales significativos que puedan afectar esta Salvaguarda.	NO APLICABLE	NO APLICABLE
3	3.8	Datos	Identificar	Flujos de datos de documentos	Flujos de Datos de Documentos. La documentación del flujo de Datos incluye los flujos de Datos del proveedor de servicios y debe basarse en el proceso de gestión de Datos de la empresa. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar esta Salvaguarda.		X
3	3.9	Datos	Proteger	Cifrar datos en medios extraíbles	Cifrar datos en medios extraíbles.	NO APLICABLE	NO APLICABLE
3	3.10	Datos	Proteger	Cifre datos confidenciales en tránsito	Cifre datos confidenciales en tránsito. Las implementaciones de ejemplo pueden incluir: Transport Layer Security (TLS) y Open Secure Shell (OpenSSH).	X	X
3	3.11	Datos	Proteger	Cifre datos confidenciales en reposo	Cifrar datos confidenciales en reposo en servidores, aplicaciones y bases de datos que contienen datos confidenciales. El cifrado de la capa de almacenamiento, también conocido como cifrado del lado del servidor, cumple con el requisito mínimo de esta Protección. Los métodos de cifrado adicionales pueden incluir cifrado en la capa de aplicación, también conocido como cifrado del lado del cliente, donde el acceso a los dispositivos de almacenamiento de Datos no permite el acceso a los Datos en texto sin formato.	X	X
3	3.12	Network	Proteger	Segmentar el procesamiento y almacenamiento de datos según la sensibilidad	Segmentar el procesamiento y almacenamiento de Datos en función de la sensibilidad de los Datos. No procese Datos confidenciales en activos empresariales destinados a Datos de menor sensibilidad.	X	X
3	3.13	Datos	Proteger	Implementar una solución de prevención de pérdida de datos	Implementar una herramienta automatizada, como una herramienta de Prevención de pérdida de datos (DLP) basada en host para identificar todos los datos confidenciales almacenados, procesados o transmitidos a través de los activos de la empresa, incluidos aquellos ubicados en el sitio o en un proveedor de servicios remoto, y actualizar los datos confidenciales de la empresa, inventario.		X
3	3.14	Datos	Detectar	Registrar acceso a datos confidenciales	Registrar el acceso a Datos confidenciales, incluida su modificación y eliminación.		X
4	**Configuración segura de activos y software empresariales**						
Establecer y mantener la configuración segura de los activos empresariales (Dispositivos de usuario final, incluidos dispositivos portátiles y móviles; Dispositivos de red; Dispositivos no informáticos/IoT; y servidores) y software (sistemas operativos y aplicaciones). Establecer y mantener la configuración segura de los activos empresariales (dispositivos de usuario final, incluidos portátiles y móviles; dispositivos de red; dispositivos no informáticos/IoT; y servidores) y software (sistemas operativos y aplicaciones).							
4	4.1	Aplicaciones	Proteger	Establecer y mantener un proceso de configuración seguro	Establecer y mantener un proceso de configuración seguro para los activos empresariales (Dispositivos de usuario final, incluidos dispositivos portátiles y móviles, no informáticos/IoT y servidores) y software (sistemas operativos y aplicaciones). Revisar y actualizar la documentación anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar esta Salvaguarda.		X
4	4.2	Network	Proteger	Establecer y mantener un proceso de configuración seguro para la infraestructura de red	Establecer y mantener un proceso de configuración seguro para la red Dispositivos. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar esta Salvaguarda.	X	X
4	4.3	Users	Proteger	Configurar el bloqueo automático de sesiones en activos empresariales	Configure el bloqueo automático de sesiones en los activos empresariales después de un período definido de inactividad. Para sistemas operativos de propósito general, el período no debe exceder los 15 minutos. Para Dispositivos de usuario final móvil, el período no debe exceder los 2 minutos.	X	X
4	4.4	Dispositivos	Proteger	Implementar y administrar un firewall en servidores	Implementar y administrar un firewall en los servidores, cuando sea compatible. Las implementaciones de ejemplo incluyen un firewall virtual, un firewall del sistema operativo o un agente de firewall de terceros.	X	X
4	4.5	Dispositivos	Proteger	Implementar y administrar un firewall en dispositivos de usuario final	Implemente y administre un firewall basado en host o una herramienta de filtrado de puertos en los Dispositivos del usuario final, con una regla de denegación predeterminada que elimine todo el tráfico excepto aquellos servicios y puertos que están explícitamente permitidos.	X	X
4	4.6	Network	Proteger	Administre de forma segura los activos y el software empresarial	Administre de forma segura los activos y el software empresarial. Las implementaciones de ejemplo incluyen la gestión de la configuración a través de infraestructura como código controlada por versión y el acceso a interfaces administrativas a través de protocolos de red seguros, como Secure Shell (SSH) y Hypertext Transfer Protocol Secure (HTTPS). No utilice protocolos de gestión inseguros, como Telnet (Teletype Network) y HTTP, a menos que sea esencial desde el punto de vista operativo.	NO APLICABLE	NO APLICABLE
4	4.7	Users	Proteger	Administrar cuentas predeterminadas en software y activos empresariales	Administre cuentas predeterminadas en activos y software empresariales, como cuentas raíz, de administrador y otras cuentas de proveedores preconfiguradas. Las implementaciones de ejemplo pueden incluir: deshabilitar cuentas predeterminadas o hacerlas inutilizables.	X	X
4	4.8	Dispositivos	Proteger	Desinstalar o deshabilitar servicios innecesarios en software y activos empresariales	Desinstale o deshabilite servicios innecesarios en activos y software de la empresa, como un servicio de intercambio de archivos, un módulo de aplicación web o una función de servicio no utilizados.	X	X
4	4.9	Dispositivos	Proteger	Configurar servidores DNS confiables en activos empresariales	Configure servidores DNS confiables en activos empresariales. Las Implementaciones de ejemplo incluyen: configuración de activos para utilizar servidores DNS controlados por la empresa y/o servidores DNS acreditados accesibles externamente.	X	X
4	4.10	Dispositivos	Responder	Aplicar el bloqueo automático de dispositivos en dispositivos portátiles de usuario final	Aplicar el bloqueo automático de dispositivos siguiendo un umbral predeterminado de intentos fallidos de autenticación local en Dispositivos portátiles de usuario final, cuando sea compatible. Para portátiles, no permita más de 20 intentos fallidos de autenticación; para tabletas y teléfonos inteligentes, no más de 10 intentos fallidos de autenticación. Las implementaciones de ejemplo incluyen Microsoft® InTune Device Lock y Apple® Configuration Profile maxFailedAttempts.	NO APLICABLE	NO APLICABLE
4	4.11	Dispositivos	Proteger	Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final	Borre de forma remota los Datos empresariales de los Dispositivos portátiles de usuario final de propiedad de la empresa cuando se considere apropiado, como Dispositivos perdidos o robados, o cuando un individuo ya no brinde soporte a la empresa.	NO APLICABLE	NO APLICABLE
4	4.12	Dispositivos	Proteger	Espacios de trabajo empresariales separados en dispositivos móviles de usuario final	Asegúrese de que se utilicen espacios de trabajo empresariales separados en los dispositivos móviles de los usuarios finales, cuando sea compatible. Las implementaciones de ejemplo incluyen el uso de un perfil de configuración de Apple® o un perfil de trabajo de Android™ para separar las aplicaciones y datos empresariales de las aplicaciones y datos personales.	NO APLICABLE	NO APLICABLE
5	**Administración de cuentas**						
Utilice procesos y herramientas para asignar y administrar autorizaciones a credenciales para cuentas de usuario, incluidas cuentas de administrador, así como cuentas de servicio, para activos y software empresariales.							

5	5.1	Users	Identificar	Establecer y mantener un inventario de cuentas	Establecer y mantener un inventario de todas las cuentas administradas en la empresa. El inventario debe incluir cuentas de usuario y de administrador. El inventario, como mínimo, debe contener el nombre de la persona, nombre de usuario, fechas de inicio/finalización y departamento. Validar que todas las cuentas activas estén autorizadas, de forma recurrente como mínimo trimestralmente o con mayor frecuencia.	X	X
5	5.2	Users	Proteger	Utilice contraseñas únicas	Utilice contraseñas únicas para todos los activos de la empresa. La implementación de mejores prácticas incluye, como mínimo, una contraseña de 8 caracteres para cuentas que usan MFA y una contraseña de 14 caracteres para cuentas que no usan MFA.	X	X
5	5.3	Users	Responder	Deshabilitar cuentas inactivas	Elimine o deshabilite cualquier cuenta inactiva después de un período de 45 días de inactividad, cuando sea posible.	X	X
5	5.4	Users	Proteger	Restringir los privilegios de administrador a cuentas de administrador dedicadas	Restrinja los privilegios de administrador a cuentas de administrador dedicadas en activos empresariales. Realizar actividades informáticas generales, como navegación por Internet, correo electrónico y uso del paquete de productividad, desde la cuenta principal sin privilegios del usuario.	X	X
5	5.5	Users	Identificar	Establecer y mantener un inventario de cuentas de servicio	Establecer y mantener un inventario de cuentas de servicios. El inventario, como mínimo, debe contener el propietario del departamento, la fecha de revisión y el propósito. Realice revisiones de cuentas de servicio para validar que todas las cuentas activas estén autorizadas, en un cronograma recurrente como mínimo trimestralmente o con mayor frecuencia.	X	X
5	5.6	Users	Proteger	Centralizar la gestión de cuentas	Centralice la gestión de cuentas a través de un directorio o servicio de identidad.		X
6				**Gestión de control de acceso**			
					Utilice procesos y herramientas para crear, asignar, administrar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio para activos y software empresariales. Utilice procesos y herramientas para crear, asignar, administrar y revocar credenciales de acceso y privilegios para cuentas de usuario, administrador y servicio para activos y software empresariales.		
6	6.1	Users	Proteger	Establecer un proceso de concesión de acceso	Establecer y seguir un proceso, preferiblemente automatizado, para otorgar acceso a los activos de la empresa tras una nueva contratación, concesión de derechos o cambio de rol de un usuario.	X	X
6	6.2	Users	Proteger	Establecer un proceso de revocación de acceso	Establecer y seguir un proceso, preferiblemente automatizado, para revocar el acceso a los activos de la empresa, mediante la desactivación de cuentas inmediatamente después de la terminación, revocación de derechos o cambio de rol de un usuario. Puede ser necesario deshabilitar cuentas, en lugar de eliminarlas, para preservar los registros de auditoría.	X	X
6	6.3	Users	Proteger	Requerir MFA para aplicaciones expuestas externamente	Solicitar MFA para aplicaciones expuestas externamente		X
6	6.4	Users	Proteger	Require MFA for Remote Network Access	Require MFA for remote network access.		X
6	6.5	Users	Proteger	Requerir MFA para acceso administrativo	Exija MFA para todas las cuentas de acceso administrativo, cuando sea compatible, en todos los activos empresariales, ya sea administrados en el sitio o a través de un proveedor externo.		X
6	6.6	Users	Identificar	Establecer y mantener un inventario de sistemas de autenticación y autorización.	Establecer y mantener un inventario de los sistemas de autenticación y autorización de la empresa, incluidos aquellos alojados en el sitio o en un proveedor de servicios remoto. Revisar y actualizar el inventario, como mínimo, anualmente o con mayor frecuencia.		X
6	6.7	Users	Proteger	Centralizar el control de acceso	Centralice el control de acceso para todos los activos empresariales a través de un servicio de directorio o proveedor de SSO, cuando sea compatible.		X
6	6.8	Datos	Proteger	Definir y mantener el control de acceso basado en roles	Defina y mantenga el control de acceso basado en roles, mediante la determinación y documentación de los derechos de acceso necesarios para que cada rol dentro de la empresa lleve a cabo con éxito sus tareas asignadas. Realice revisiones de control de acceso de los activos empresariales para validar que todos los privilegios estén autorizados, en un cronograma recurrente como mínimo anualmente o con mayor frecuencia.		X
7				**Gestión continua de vulnerabilidades**			
					Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la empresa, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes. Supervise las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades. Desarrollar un plan para evaluar y rastrear continuamente las vulnerabilidades en todos los activos empresariales dentro de la infraestructura de la empresa, con el fin de remediar y minimizar la ventana de oportunidad para los atacantes. Supervise las fuentes de la industria pública y privada en busca de nueva información sobre amenazas y vulnerabilidades.		
7	7.1	Aplicaciones	Proteger	Establecer y mantener un proceso de gestión de vulnerabilidades	Establecer y mantener un proceso documentado de gestión de vulnerabilidades para los activos empresariales. Revisar y actualizar la documentación anualmente o cuando se produzcan cambios empresariales importantes que puedan afectar esta Salvaguarda.		X
7	7.2	Aplicaciones	Responder	Establecer y mantener un proceso de remediación	Establecer y mantener una estrategia de remediación basada en riesgos documentada en un proceso de remediación, con revisiones mensuales o más frecuentes.		X
7	7.3	Aplicaciones	Proteger	Perform Automated Operating System Patch Management	Realizar una gestión automatizada de parches del sistema operativo		X
7	7.4	Aplicaciones	Proteger	Realice una gestión automatizada de parches de aplicaciones	Realice actualizaciones de aplicaciones en activos empresariales a través de la gestión automatizada de parches mensualmente o con mayor frecuencia.		X
7	7.5	Aplicaciones	Identificar	Realice análisis automatizados de vulnerabilidades de los activos internos de la empresa	Realice análisis automatizados de vulnerabilidades de los activos internos de la empresa trimestralmente o con mayor frecuencia. Realice análisis autenticados y no autenticados utilizando una herramienta de análisis de vulnerabilidades compatible con SCAP.		X
7	7.6	Aplicaciones	Identificar	Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets	Realice análisis automatizados de vulnerabilidades de activos empresariales expuestos externamente.		X
7	7.7	Aplicaciones	Responder	Remediar vulnerabilidades detectadas	Remediar las vulnerabilidades detectadas en el software a través de procesos y herramientas mensualmente o con mayor frecuencia, según el proceso de remediación.		X
9				**Protección del correo electrónico y del navegador web**			
					Mejore las protecciones y detecciones de amenazas provenientes del correo electrónico y los vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano a través del compromiso directo. Mejore las protecciones y detecciones de amenazas provenientes del correo electrónico y los vectores web, ya que estas son oportunidades para que los atacantes manipulen el comportamiento humano mediante el compromiso directo.		
9	9.1	Aplicaciones	Proteger	Garantice el uso únicamente de navegadores y clientes de correo electrónico totalmente compatibles	Asegúrese de que solo los navegadores y clientes de correo electrónico totalmente compatibles puedan ejecutarse en la empresa, utilizando únicamente la última versión de los navegadores y clientes de correo electrónico proporcionada a través del proveedor.		X
9	9.2	Network	Proteger	Utilice servicios de filtrado DNS	Utilice servicios de filtrado DNS en todos los activos empresariales para bloquear el acceso a dominios maliciosos conocidos.	X	X
9	9.3	Network	Proteger	Mantener y aplicar filtros de URL basados en la red	Mantener y aplicar filtros de URL basados en la red	X	X
9	9.3	Network	Proteger	Mantener y aplicar filtros de URL basados en la red	Aplique y actualice filtros de URL basados en la red para limitar la conexión de un activo empresarial a sitios web potencialmente maliciosos o no aprobados. Las implementaciones de ejemplo incluyen el filtrado basado en categorías, el filtrado basado en reputación o mediante el uso de listas de bloqueo. Aplique filtros para todos los activos empresariales.	X	X
9	9.4	Aplicaciones	Proteger	Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	Restringir, ya sea desinstalando o deshabilitando, cualquier complemento, extensión y aplicación complementaria no autorizada o innecesaria del navegador o del cliente de correo electrónico.		X

9	9.5	Network	Proteger	Implementar DMARC	Para reducir la posibilidad de correos electrónicos falsificados o modificados de dominios válidos, implemente la política y verificación DMARC, comenzando por implementar los estándares Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM).		X
9	9.6	Network	Proteger	Bloquear tipos de archivos innecesarios	Bloquee tipos de archivos innecesarios que intenten ingresar al portal de correo electrónico de la empresa.		X
9	9.7	Network	Proteger	Implementar y mantener protecciones antimalware del servidor de correo electrónico	Implementar y mantener protecciones antimalware del servidor de correo electrónico, como escaneo de archivos adjuntos y/o zona de pruebas.	X	X

26/02/2024

Gerente de Sistemas

Edison Sanchez

Anexo 4: Informe de controles CIS v.8 implementados en el servicio de comunicación asíncrona de Comercial Hidrobo S.A.

APLICACIÓN DE CONTROLES CIS

Control 1 Inventario y Control de activos de hardware

1.1 Establecer y mantener un inventario detallado de activos empresariales

El inventario se realizó y se encuentra presentado a la empresa.

1.2 Abordar activos no autorizados

Proceso para abordar activos no autorizados:

-Los equipos que se conectan a la red de wifi llamada invitados, tienen libre acceso al internet, manteniendo las reglas de las listas negras y listas blancas de navegación configurada en el cortafuegos y en el servicio Postfix.

-Los equipos que se conectan a nuestra red vía ethernet requieren autorización para asignarles una Ip estática y poder navegar libremente.

Diagrama de proceso:

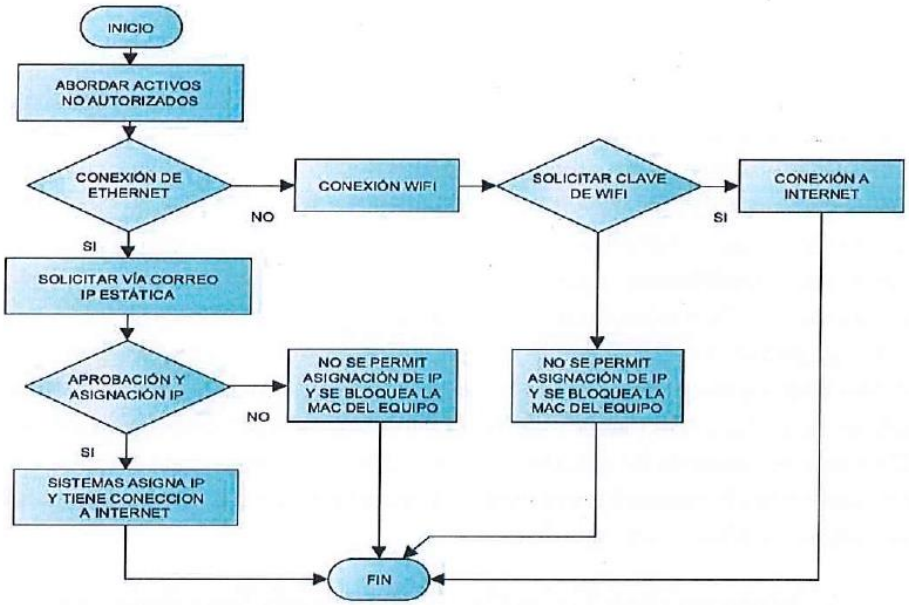


Figura 1 Proceso para abordar activos no autorizados. Fuente: Autor

1.3 Utilice una herramienta de descubrimiento activo.

La herramienta que se usa es Nmap la cual nos detalla los puertos junto con los servicios que están activos, se procede a configurar esta herramienta para que realice un escaneo diario generando un reporte el cual se generará en un directorio específico.

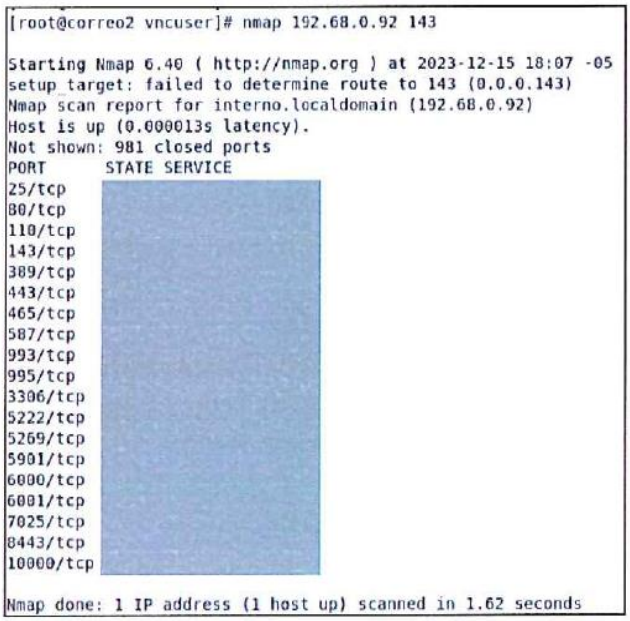


Figura 2 Escaneo con Nmap. Fuente: Autor

1.4 Utilice el registro del Protocolo de configuración dinámica de host (DHCP) para actualizar el inventario de activos empresariales.

En el entorno operativo, se gestiona los equipos utilizando direcciones IP estáticas. Esta elección estratégica brinda mayor control y estabilidad en la asignación de direcciones a cada dispositivo en la red. Al emplear direcciones IP estáticas, se asegura una identificación constante y predecible para cada equipo, facilitando la administración y la resolución de problemas. Esta práctica también se traduce en una mayor seguridad al minimizar la exposición a posibles amenazas asociadas con cambios dinámicos de direcciones. En resumen, la implementación de direcciones IP estáticas optimiza la eficiencia y confiabilidad de nuestra infraestructura tecnológica.

1.5 Utilice una herramienta de descubrimiento pasivo de activos.

Se procede usando comandos del mismo sistema operativo. Usando comandos como nslookup se verifica el servidor de correo

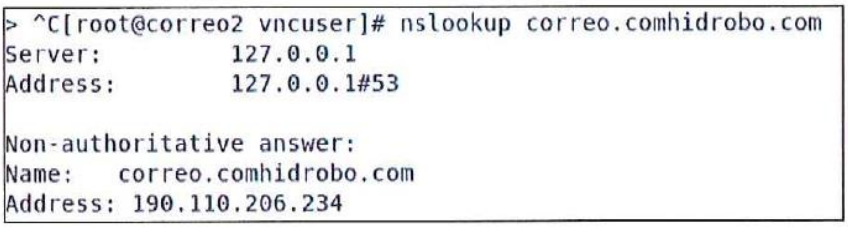


Figura 3 Nslookup Fuente: Autor

Continuando con la verificación del certificado del dominio

Figura 4 Continuación del comando Nslookup Fuente: Autor

Finalmente, para determinar qué información existe sobre las áreas del sitio web que los propietarios prefieren que no sean rastreadas por motores de búsqueda, así como otras directrices específicas para los bots.

```
[root@correo2 vncuser]# curl google.com/robots.txt
<HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="https://www.google.com/robots.txt">here</A>.
</BODY></HTML>
```

Figura 5 Configuración de robots de búsqueda. Fuente: Autor

Figura 6 Demostración de que la pagina robots no existe en el dominio Fuente:Autor

Control 2 Inventario y Control de activos de software

2.1 Establecer y mantener un inventario detallado de activos empresariales.
El inventario se realizó y se encuentra presentado a la empresa.

2.2 Asegúrese de que el software autorizado sea actualmente compatible
Dentro del inventario de activos de software de la empresa se registra las versiones y se determina que sean actuales y compatibles.

Con una exploración diaria revisando las actualizaciones disponibles tanto del sistema operativo como de las aplicaciones que contiene, se mantienen actualizadas las versiones.

2.3 Abordar el software no autorizado

Dentro del servidor, el antivirus desempeña un papel fundamental al notificar al administrador mediante correo electrónico sobre la presencia de software no autorizado. Esta función proactiva permite al administrador estar al tanto de posibles amenazas o vulnerabilidades en tiempo real. Ante tales notificaciones, el administrador lleva a cabo una revisión exhaustiva de las aplicaciones detectadas, identificando aquellas que no cuentan con la debida autorización. Posteriormente, toma medidas inmediatas para eliminar o desactivar estas aplicaciones no autorizadas, asegurando así la integridad y la seguridad de nuestro sistema. Este enfoque proactivo y reactivo garantiza un entorno informático más robusto y protegido contra posibles riesgos cibernéticos.

2.4 Utilice herramientas de inventario de software automatizadas

El mismo sistema operativo proporciona comandos para realizar un inventario del software instalado, es así que se puede generar un archivo plano con este listado, permitiendo verificarlo.

2.5 Software autorizado en la lista de permitidos

El antivirus maneja un listado de aplicaciones permitidas, el mismo notifica al administrador cuando se intenta ejecutar aplicaciones que no se encuentran en esa lista o considera maliciosas. Una vez notificado se procede con la revisión y eliminación de la aplicación en cuestión.

2.6 Lista de bibliotecas autorizadas permitidas no aplica

En el servidor de correo electrónico que gestionamos, es importante señalar que no se aplica un control específico mediante una lista de bibliotecas autorizadas permitidas. A diferencia de otros aspectos de nuestro sistema, donde se implementan medidas de seguridad detalladas, en este contexto no hemos optado por restringir explícitamente el acceso a bibliotecas específicas. La decisión de no aplicar esta lista se basa en la flexibilidad necesaria para adaptarnos a las diversas necesidades de nuestros usuarios y permitir un intercambio de información eficiente. No obstante, se mantienen otras capas de seguridad y controles para preservar la integridad y confidencialidad de los datos que circulan a través del servidor de correo electrónico.

2.7 Lista de scripts autorizados permitidos

En el servidor de correo electrónico que administramos, es relevante destacar que no se implementa un control específico mediante una lista de scripts autorizados permitidos. A diferencia de ciertos protocolos de seguridad que restringen el uso de scripts específicos, hemos optado por una política más abierta para ofrecer flexibilidad y adaptabilidad a las necesidades cambiantes de nuestros usuarios. La decisión de no aplicar esta lista se centra en facilitar el intercambio de información y

en permitir a los usuarios utilizar scripts según sus requerimientos particulares. Sin embargo, es importante subrayar que se mantienen otras medidas de seguridad integrales en el servidor para garantizar la protección y confidencialidad de los datos que circulan a través del sistema de correo electrónico.

Control 3 Establecer y mantener un proceso de gestión de datos

3.1 Establecer y mantener un proceso de gestión de datos.

La solicitud de creación de un correo electrónico es solicitada por RRHH vía intranet, una vez así, se ingresa la información necesaria en el administrador de correo directamente con el usuario final, la información solicitada es: 1 nombre, 1 apellido, Una Inicial del 2do nombre y una contraseña, el formato empresarial del correo electrónico se establece con la inicial del primer nombre junto con el primer apellido seguido del @ y dominio correspondiente, se solicita una contraseña alfanumérica de mínimo 8 dígitos.
Diagrama de proceso:

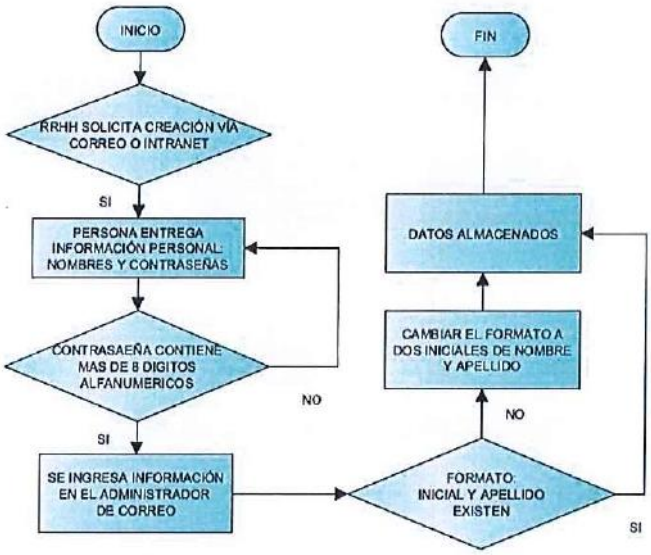


Figura 7 Proceso de gestión de datos. Fuente: Autor

3.2 Establecer y mantener un inventario de datos.

Se ha realizado un inventario de datos del correo electrónico, el cual fue presentado a la empresa.

3.3 Configurar listas de control de acceso a datos (listas blancas).

La configuración de la lista negra (blacklist) se encuentra en el directorio de configuración del servidor, específicamente en un archivo plano que alberga un listado de direcciones IP y dominios catalogados como maliciosos. Además de esta configuración global, cada cuenta de correo electrónico posee una configuración individual que permite a los usuarios bloquear o permitir dominios y cuentas de correo específicas. Esta funcionalidad individualiza el control de acceso y se asemeja a una lista negra y blanca personalizada para cada cuenta, proporcionando a los

usuarios un nivel adicional de personalización y seguridad en la gestión de sus correos electrónicos.

3.4 Hacer cumplir la retención de datos.

El tiempo de retención de una cuenta activa depende del tiempo que el colaborador está en la empresa y que cargo desempeño en la misma, en el caso de que fuese un cargo importante y que se haya usado esa cuenta para registrar en algún servicio importante, esta cuenta se mantiene hasta que se registre una nueva cuenta en ese servicio como máximo en 360 días, caso contrario si el usuario no tuvo ninguna relación importante en servicios, la cuenta queda bloqueada y posteriormente es eliminada en 30 días de su salida de la empresa.

Diagrama de proceso:

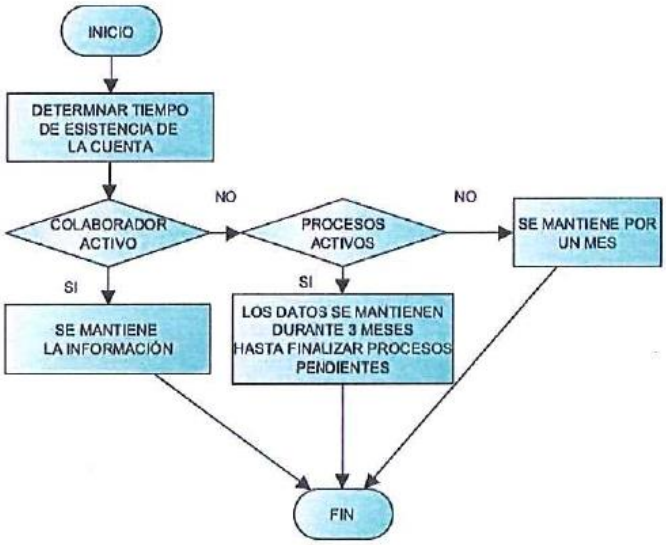


Figura 8 Proceso retención de datos.

3.5 Eliminar datos de forma segura.

Por correo electrónico o intranet solicitar la eliminación de una cuenta de correo electrónico una vez que sea aprobada por gerencia general o gerencia de sistemas y así el proceso se cumpla a cabalidad.

Diagrama de proceso:

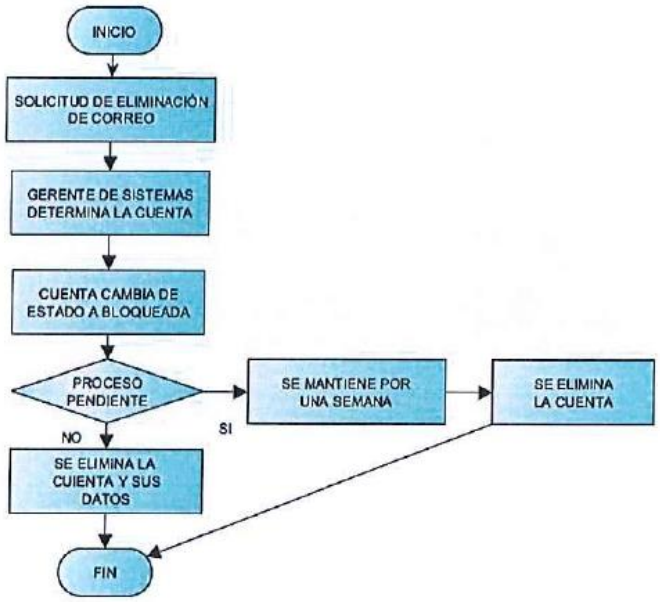


Figura 9 Proceso de eliminación de datos de forma segura. Fuente: Autor

3.6 Cifrar datos en dispositivos de usuario final.

La decisión de no aplicar un control específico para cifrar datos en dispositivos de usuario final en nuestro servicio de correo electrónico se fundamenta en la búsqueda de un equilibrio entre seguridad y accesibilidad. Si bien el cifrado de datos es una medida efectiva para proteger la confidencialidad de la información, su implementación en dispositivos de usuario final puede resultar en una experiencia de usuario más compleja y potencialmente menos accesible. La prioridad es garantizar que nuestros usuarios puedan acceder y gestionar sus correos electrónicos de manera eficiente, sin obstáculos innecesarios. En lugar de imponer un cifrado en los dispositivos de usuario final, nos enfocamos en otras capas de seguridad y controles en el servidor, asegurando la integridad de la comunicación y protegiendo los datos durante su tránsito a través de la red. Esta estrategia busca proporcionar un equilibrio adecuado entre la protección de la información y la usabilidad del servicio.

3.7 Establecer y mantener un esquema de clasificación de datos

Optamos por no implementar un esquema de clasificación de datos en nuestro servicio de correo electrónico para simplificar la experiencia del usuario y facilitar la interacción sin añadir complejidades innecesarias. Aunque la clasificación puede ser útil para la gestión de la información, priorizamos la simplicidad y la eficiencia, manteniendo medidas de seguridad efectivas a través de otros controles en el servidor.

3.8 Flujos de datos de documentos

Representación gráfica y genérica del flujo de documentos

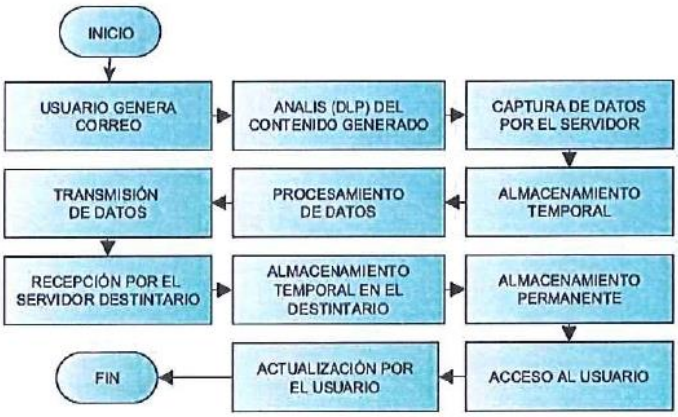


Figura 10 Flujo de documentos de dados. Fuente: Autor

3.9 Cifrar datos en medios extraíbles

El control de cifrado de datos en medios extraíbles puede no ser directamente aplicable al servidor de correo electrónico, ya que la naturaleza de este control se centra en asegurar la información almacenada en dispositivos portátiles, como USB o discos externos. Los servidores de correo electrónico, por otro lado, gestionan el flujo de mensajes electrónicos y no almacenan datos de manera física en medios extraíbles. Si bien la seguridad en el entorno de correo electrónico es esencial, las medidas específicas pueden diferir de aquellas necesarias para proteger datos almacenados en dispositivos portátiles. En lugar de enfocarse en el cifrado de medios extraíbles, los servidores de correo electrónico deben implementar prácticas de cifrado de extremo a extremo, autenticación segura y otras medidas específicas para salvaguardar la confidencialidad e integridad de los mensajes transmitidos a través de la red.

3.10 Cifrar datos confidenciales en tránsito

Se ha implementado el control de cifrado de datos confidenciales en tránsito mediante la configuración de Transport Layer Security (TLS) para salvaguardar la integridad y confidencialidad de la información durante su transmisión a través de la red. La implementación de TLS asegura que los mensajes de correo electrónico viajen de manera cifrada entre los servidores de correo y los clientes, protegiéndolos de posibles accesos no autorizados. Además, se ha fortalecido la seguridad del servidor mediante la implementación de Open Secure Shell (OpenSSH), proporcionando una conexión segura y cifrada para la administración remota del servidor. Estas medidas combinadas no solo garantizan la privacidad de los datos confidenciales transmitidos a través del servidor de correo electrónico, sino que también refuerzan la seguridad general del sistema al incorporar prácticas seguras de comunicación y administración.

3.11 Cifrar datos confidenciales en reposo

Al aplicar certificados SSL/TLS en el servidor, se establece una capa adicional de protección para los datos en reposo, ya que estos certificados cifran la comunicación entre clientes y servidores, así como entre los diversos componentes internos del sistema. Esta medida no solo asegura la confidencialidad de los datos durante su transmisión, sino que también contribuye a la integridad y seguridad de los datos almacenados en el repositorio del servidor. Los certificados SSL/TLS garantizan que

la información sensible se encuentre resguardada, mitigando el riesgo de accesos no autorizados y asegurando la privacidad de los datos almacenados en el entorno del servidor.

3.12 Segmentar el procesamiento y almacenamiento de datos según la sensibilidad

La empresa ha establecido una sólida política de seguridad de datos que abarca medidas específicas para salvaguardar el procesamiento y almacenamiento de información en el servidor de correo electrónico. Este enfoque garantiza la protección integral de los datos, abordando tanto la seguridad durante el manejo como durante el almacenamiento, fortaleciendo así la integridad y confidencialidad de la información crítica para la organización.

3.13 Implementar una solución de prevención de pérdida de datos

Implementar un DLP el antivirus cuenta con un DLP el cual estamos en proceso de configuración para su implementación.

3.14 Registrar acceso a datos confidenciales

Este proceso implica obtener autorización a través de correo electrónico por parte de un superior. Él solicitará formalmente, también por correo electrónico, al departamento de sistemas la configuración pertinente para el acceso de datos. Es fundamental destacar que el acceso estará sujeto a un monitoreo continuo por parte del departamento de sistemas, con el objetivo de prevenir cualquier alteración no autorizada en los datos. Este proceso puede ser permanente una sola vez se configura y solicita o temporal repetir el proceso cada vez que se requiera.

Diagrama de procesos:

Figura 11 Proceso registrar acceso a datos confidenciales. Fuente: Autor

Control 4 Configuración segura de activos y software empresariales

4.1 Establecer y mantener un proceso de configuración seguro

Se presenta a continuación un diagrama de procesos que detalla la configuración segura implementada en el servidor de correo. Este visual proporciona una visión clara

y concisa de las distintas etapas y medidas adoptadas para asegurar la integridad y confidencialidad de la información que fluye a través del sistema.

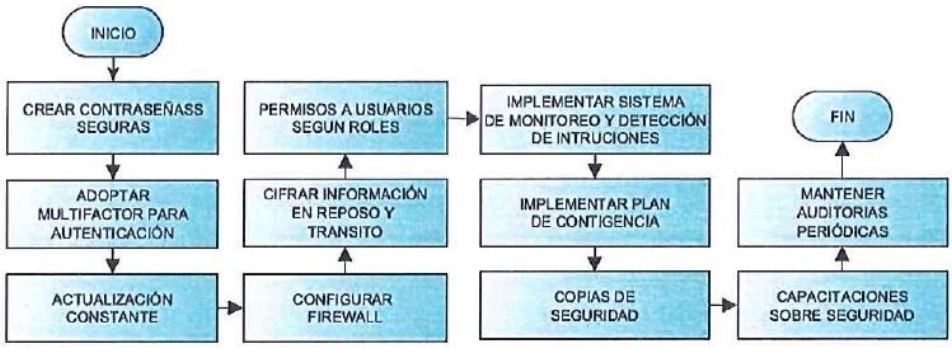


Figura 12 Proceso de configuración seguro. Fuente: Autor

4.2 Establecer y mantener un proceso de configuración seguro para la infraestructura de red.

Instalación de un servidor de dominio y configuración de roles y características, así como establecer un Active Directory, es una práctica recomendada para optimizar la administración y seguridad de una red. Al implementar un servidor de dominio, es posible centralizar la gestión de usuarios, dispositivos y recursos, simplificando tareas como la asignación de permisos y la aplicación de políticas de seguridad.

Figura 13 Proceso de configuración seguro para la infraestructura de red. Fuente: Autor

4.3 Configurar el bloqueo automático de sesiones en activos empresariales

Se ha establecido una medida de seguridad efectiva mediante la configuración del bloqueo automático, el cual entra en funcionamiento después de un periodo de inactividad de 5 minutos en las sesiones de administradores. Esta precaución

contribuye significativamente a la protección de la información sensible y a la prevención de accesos no autorizados.

4.4 Implementar y administrar un firewall en servidores

Actualmente existe un software configurado que trabaja como firewall para la administración del servidor de correos. El software llamado (Firewalld proporciona un cortafuegos gestionado dinámicamente con soporte para zonas de red/fuego que definen el nivel de confianza de las conexiones de red o interfaces. Tiene soporte para la configuración de firewall IPv4, IPv6, puentes ethernet y conjuntos IP. Hay una separación de las opciones de tiempo de ejecución y configuración permanente. También proporciona una interfaz para servicios o aplicaciones para agregar directamente las reglas del cortafuegos.) (firewalld, 2023)

También cuenta con un firewall perimetral físico Gaia R80.40 que está configurado con las especificaciones necesarias para la organización, lo que nos permite una mejor prevención de amenazas a la red y mayor solución ante posibles intrusiones.

4.5 Implementar y administrar un firewall en dispositivos de usuario final

Actualmente se usa la configuración por default de firewall de Windows, no es lo más recomendable ya que puede ser una ventaja para atacantes cibernéticos. Se procede con una configuración avanzada para cada equipo en la empresa, la misma que permite asegurar la navegación y uso de los equipos.

4.6 Administre de forma segura los activos y el software empresarial

La implementación del control para administrar de forma segura los activos y el software empresarial no es aplicable a nuestra empresa en este momento. Esta decisión se basa en la evaluación de nuestras necesidades específicas y en la consideración de factores como el tamaño de la organización, la naturaleza de nuestros activos y la estructura de nuestro software. Aunque este control puede ser crucial en otros contextos, hemos determinado que nuestras actuales prácticas y protocolos de gestión de activos y software son efectivos y adecuados para mantener la seguridad y eficiencia operativa en nuestra empresa. Este enfoque nos permite optimizar nuestros recursos y adaptarnos de manera más precisa a las particularidades de nuestro entorno empresarial.

4.7 Administrar cuentas predeterminadas en software y activos empresariales

Se ha implementado una medida de seguridad fundamental en nuestros software y activos empresariales: la ausencia de cuentas predeterminadas. En lugar de depender de cuentas preexistentes que puedan representar un riesgo potencial, todos los usuarios asociados con estos sistemas han sido creados de manera específica. Esto garantiza que no haya cuentas predeterminadas activas, reduciendo significativamente el riesgo de accesos no autorizados y fortaleciendo la seguridad de nuestros activos empresariales. Esta práctica refleja nuestro compromiso con la mitigación proactiva de riesgos y la protección de la integridad de nuestros sistemas.

4.8 Desinstalar o deshabilitar servicios innecesarios en software y activos empresariales.

Una vez realizado una revisión de todos los servicios instalados se percata de los innecesarios y se procede con la eliminación. Se muestra el proceso en la siguiente ilustración:

Figura 14 Proceso desinstalar o deshabilitar servicios innecesarios en software y activos empresariales. Fuente: Autor

4.9 Configurar servidores DNS confiables en activos empresariales

Con el objetivo de optimizar la conectividad y el rendimiento de todos los activos de nuestra empresa, la empresa decidió implementar los servidores DNS proporcionados por el proveedor de servicios de Internet. Esta medida estratégica busca mejorar la velocidad de acceso a recursos en línea, fortalecer la seguridad de las comunicaciones y garantizar una gestión eficiente de las conexiones en toda la red corporativa. Al estandarizar el uso de los DNS de nuestro proveedor, esperamos lograr una mayor coherencia en la resolución de nombres de dominio y, en consecuencia, elevar la eficacia general de nuestras operaciones digitales.

4.10 Aplicar el bloqueo automático de dispositivos en dispositivos portátiles de usuario final

La razón por la cual no implementamos el control en cuestión radica en la escasa presencia de dispositivos portátiles en nuestra empresa. Dado que el número de estos dispositivos es limitado, hemos evaluado que la aplicación específica de este control no se justifica en nuestro contexto operativo actual. Nuestra decisión se orienta a optimizar los recursos y las prácticas de seguridad de manera proporcional a las necesidades específicas de nuestra infraestructura empresarial, enfocándonos en medidas más adecuadas a nuestra realidad operativa.

4.11 Aplicar la capacidad de borrado remoto en dispositivos portátiles de usuario final

La aplicación de la capacidad de borrado remoto en dispositivos portátiles de usuario final se considera un control no aplicable dentro de nuestra empresa por diversas razones. En primer lugar, la infraestructura y el entorno de trabajo no dependen significativamente de un gran número de dispositivos portátiles. La baja cantidad de estos dispositivos minimiza la necesidad de una funcionalidad de borrado remoto, ya que los riesgos asociados a la pérdida o robo son limitados. Además, las políticas de seguridad actuales se centran en medidas proactivas que aborden eficazmente los riesgos identificados, y en este caso, otras medidas de seguridad, como autenticación robusta y cifrado de datos, han demostrado ser suficientes para mantener la integridad de la información en dispositivos portátiles en nuestro entorno empresarial. En este contexto, la implementación de la capacidad de borrado remoto se percibe como innecesaria y no proporcionaría un beneficio proporcional a los recursos y complejidades adicionales que conllevaría.

Control 5 Administración de cuentas

5.1 Establecer y mantener un inventario de cuentas

El listado detallado del inventario ha sido completado y presentado en la empresa.

5.2 Utilice contraseñas únicas

Con el propósito de mejorar la seguridad de las cuentas de correo electrónico, se ha implementado una nueva política que exige contraseñas de al menos 8 caracteres alfanuméricos, incluyendo caracteres especiales, y que sean únicas, sin ser utilizadas en otras cuentas. Además, se ha incorporado la autenticación de múltiples factores (MFA) para proporcionar una capa adicional de seguridad durante el proceso de verificación.

5.3 Deshabilitar cuentas inactivas

Con el objetivo de reforzar la seguridad cibernética, se ha implementado una medida proactiva para eliminar las cuentas inactivas que llevan más de 45 días sin actividad. Esta práctica contribuye a mitigar posibles riesgos, ya que las cuentas inactivas durante un período prolongado pueden convertirse en vectores potenciales para ciberataques. Al eliminar estas cuentas, se reduce significativamente la superficie de ataque, fortaleciendo así las defensas contra posibles amenazas y preservando la integridad del sistema.

5.4 Restringir los privilegios de administrador a dedicados

Para fortalecer la seguridad en el servidor de correo electrónico, es fundamental restringir los privilegios de administrador a cuentas dedicadas, limitando su uso exclusivamente a tareas administrativas. Las actividades informáticas generales, como la navegación por Internet y el correo electrónico, deben realizarse desde cuentas estándar sin privilegios de administrador. Esta práctica minimiza el riesgo de posibles amenazas y ciberataques, al tiempo que se establecen políticas, monitorización y

capacitación para mantener un entorno seguro y cumplir con las mejores prácticas de seguridad informática.

5.5 Establecer y mantener un inventario de cuentas de servicios

El inventario se encuentra presentado en un archivo de Excel a la empresa.

5.6 Centralizar la gestión de cuentas

Para optimizar la administración de cuentas y fortalecer la seguridad, se recomienda implementar un control que centralice la gestión de cuentas en el entorno informático. Esta medida implica consolidar la administración de usuarios y privilegios en un sistema centralizado, facilitando la aplicación uniforme de políticas de seguridad. Al centralizar la gestión de cuentas, se logra una mayor visibilidad y control sobre los accesos, permitiendo una respuesta más efectiva a posibles amenazas y facilitando la implementación de cambios, actualizaciones y auditorías de manera más eficiente. Este enfoque integral contribuye significativamente a mantener un entorno de TI más seguro y fácil de administrar.

Control 6 Gestión de control de acceso

6.1 Establecer un proceso de concesión de acceso

Enfocándonos estrictamente en un proceso de concesión de acceso a un correo nuevo creado para el colaborador el momento de su ingreso se detalla en el siguiente gráfico

Figura 15 Proceso de concesión de acceso. Fuente:Asesor

6.2 Establecer un proceso de revocación de acceso

La cuenta procede a ser bloqueada para el acceso del usuario, pero permanece en el servidor hasta 360 días después o si es necesario se mantiene, el proceso es detallado en el siguiente gráfico:

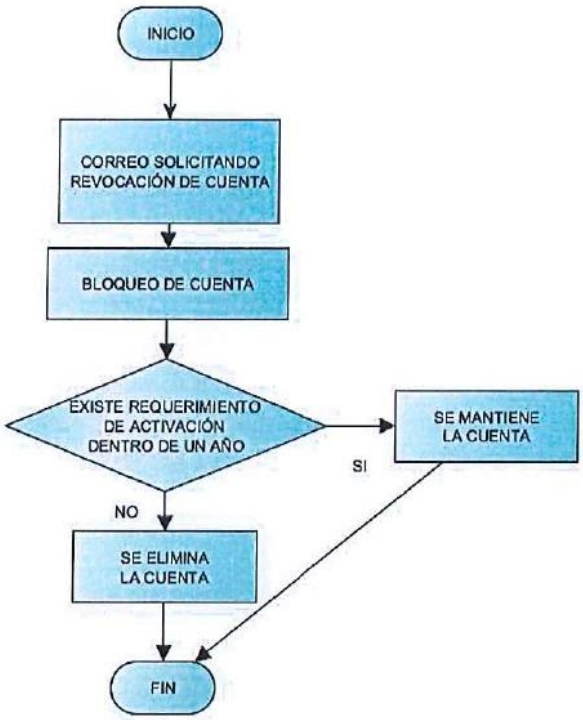


Figura 16 Proceso de revocación de acceso. Fuente: Asesor

6.3 Requerir MFA para aplicaciones expuestas externamente

El servicio de correo electrónico es un servicio que está expuesto al exterior por su característica de comunicación, actualmente está autentificación no está disponible, pero está en revisión para implementarla próximamente.

6.4 Requerir MFA para acceso remoto a la red

No existe conexión remota en la organización ya solo se trabaja en horarios laborales y no es necesario este tipo de conexión.

6.5 Requerir MFA para acceso administrativo

Actualmente está autentificación no está disponible, pero está en revisión para implementarla próximamente.

6.6 Establecer y mantener un inventario de sistemas de autenticación y autorización.

Para fortalecer la seguridad en el entorno informático, se recomienda la implementación de un sistema robusto de autenticación y autorización. Este control implica establecer un mecanismo sólido que verifique de manera segura la identidad de los usuarios antes de otorgarles acceso a los recursos del sistema. Además, se deben definir políticas claras de autorización que determinen los niveles de acceso y los privilegios asociados a cada cuenta. La combinación de autenticación y autorización proporciona una capa adicional de protección, reduciendo los riesgos de accesos no autorizados y asegurando que los usuarios solo tengan acceso a los recursos pertinentes a sus roles y responsabilidades. La implementación de este sistema contribuirá

significativamente a fortalecer la seguridad y el control en el entorno informático de manera integral.

6.7 Centralizar el control de acceso

Para optimizar la gestión y seguridad de los activos empresariales, se recomienda centralizar el control de acceso mediante la implementación de un servicio de directorio o un proveedor de Single Sign-On (SSO), siempre que sea compatible con la infraestructura existente. Este enfoque permite consolidar la administración de identidades y accesos en un único punto, simplificando la gestión y asegurando la coherencia en las políticas de seguridad. Un servicio de directorio o SSO facilita la autenticación eficiente de usuarios y la asignación consistente de privilegios, mejorando la visibilidad y control sobre el acceso a los recursos

6.8 Control de acceso basado en roles

Sería beneficioso considerar la implementación de Active Directory para centralizar el control de acceso en la empresa. Active Directory proporciona una gestión integral de identidades y accesos, simplificando la administración de usuarios y políticas de seguridad. Esta solución de Microsoft puede mejorar la eficiencia operativa y la seguridad de la red, siendo compatible con diversos servicios y aplicaciones. Implementar Active Directory podría contribuir significativamente a optimizar la administración de activos empresariales y a facilitar un entorno más cohesionado y seguro.

Control 7 Gestión continua de vulnerabilidades

7.1 Establecer y mantener un proceso de gestión de vulnerabilidades

El procedimiento para la gestión de vulnerabilidades se ilustra en el flujograma que se presenta a continuación.

Figura 17 proceso de gestión de vulnerabilidades. Fuente: Autor

7.2 Establecer y mantener un proceso de remediación

El enfoque estratégico de la empresa hacia la seguridad cibernética se evidencia claramente a través del proceso de remediación basada en riesgos, el cual se presenta detalladamente en el siguiente diagrama de flujo:

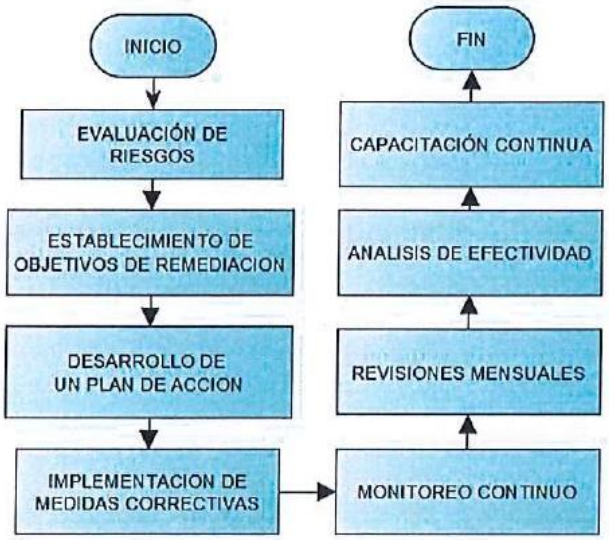


Figura 18 Proceso de remediación. Fuente: Autor

7.3 Realizar la gestión automatizada de parches del sistema operativo

Al trabajar con CentOS como sistema operativo, es posible simplificar y agilizar el proceso de actualización mediante la creación de un archivo de configuración. Esta práctica permite la automatización de las actualizaciones del sistema, asegurando que el proceso sea más eficiente y menos propenso a errores. Al establecer configuraciones específicas, se facilita la tarea de mantener el sistema operativo actualizado de manera sistemática y sin intervención manual constante, optimizando así la gestión de CentOS.

7.4 Realizar la gestión automatizada de parches de aplicaciones

Habilitar la función de autoparcheo en la herramienta de correo electrónico no solo simplifica, sino que también posibilita las actualizaciones automáticas de manera eficiente. Configurando esta característica, se establece un proceso automatizado que garantiza que la herramienta esté constantemente actualizada con las últimas mejoras y parches de seguridad disponibles. Esta práctica no solo ahorra tiempo y esfuerzo en la gestión de actualizaciones, sino que también refuerza la seguridad y el rendimiento del sistema de correo electrónico, asegurando un funcionamiento óptimo en todo momento.

7.5 Realizar análisis automatizados de vulnerabilidades internas

La herramienta Nessus que es utilizada en esta investigación es compatible con el protocolo SCAP, el cual es un conjunto de estándares que incluye formatos de datos y protocolos para automatizar la evaluación de políticas de seguridad, la monitorización de vulnerabilidades y la gestión de configuraciones de seguridad.

7.6 Realizar análisis de vulnerabilidad automatizados de objetos expuestos externamente

El informe del análisis se encuentra adjunto en los anexos, proporcionando una revisión detallada de los hallazgos y resultados obtenidos durante el proceso de evaluación.

7.7 Remediar vulnerabilidades detectadas

Este control fue realizado exitosamente, los resultados son verificados en el documento de tesis "Adopción de controles de seguridad CIS Controls v.8 basado en la Norma ISO/IEC 27001:2022 usando la metodología MAGERIT v.3 para mejorar la comunicación asíncrona de la empresa Comercial Hidrobo S.A.". (Mafla, 2024)

Control 9 Protecciones de correo electrónico y navegador web

9.1 Garantizar el uso únicamente de navegadores y clientes de correo electrónico totalmente compatibles.

Anualmente, llevamos a cabo un proceso de mantenimiento de equipos que incluye la revisión de la correcta utilización de navegadores. Aunque en la empresa se limita a tres opciones específicas: Internet Explorer, Chrome y Firefox, es importante garantizar que dichos navegadores se empleen de manera adecuada. Cabe destacar que nuestro servicio de correo es compatible con todos los navegadores comerciales, reforzando así la flexibilidad y accesibilidad para todos los usuarios.

9.2 Utilice servicios de filtrado DNS

Al utilizar los servicios de DNS proporcionados por nuestro proveedor de Internet, nos adherimos al filtro DNS configurado por dicho proveedor, lo que constituye un respaldo esencial para fortalecer la seguridad de nuestras operaciones. Esta práctica no solo optimiza la eficiencia del acceso a recursos en línea, sino que también contribuye significativamente a mitigar posibles amenazas y riesgos asociados con el filtrado de contenidos maliciosos. La alineación con la configuración de filtrado DNS del proveedor refleja nuestro compromiso con la seguridad y la protección proactiva de nuestra red.

9.3 Mantener y aplicar filtros de URL basados en red

Contamos con un firewall perimetral gestionado por nuestro proveedor de servicios de Internet, lo que nos capacita para implementar filtros específicos según nuestras necesidades. Esta infraestructura de seguridad es esencial para resguardar nuestra red contra posibles amenazas externas, garantizando un control efectivo sobre el tráfico y permitiéndonos establecer políticas de filtrado adaptadas a los requisitos de seguridad de nuestra organización. La colaboración con nuestro proveedor en la gestión de este firewall refleja nuestro compromiso continuo con la protección y la integridad de nuestros sistemas.

9.4 Restringir navegadores y correos electrónicos innecesarios o no autorizados

En el contexto de la administración de mi servidor, he implementado medidas de seguridad mediante la aplicación de controles de acceso utilizando iptables. Se establece reglas específicas que bloquean el tráfico indeseado proveniente de navegadores y clientes de correo no deseados. Con estas configuraciones, he restringido el acceso a servicios como HTTP, HTTPS y SMTP, asegurando así una capa adicional de protección contra posibles amenazas cibernéticas. Estas medidas contribuyen a fortalecer la seguridad de mi entorno de servidor al prevenir el acceso no autorizado y reducir la exposición a riesgos potenciales asociados con el tráfico web y de correo electrónico no deseado.

9.5 Implementar DMARC

En la gestión de la seguridad de la infraestructura en el servidor, se aplica medidas clave para reducir la amenaza de correos electrónicos falsificados o alterados mediante la implementación de DMARC (Domain-based Message Authentication, Reporting, and Conformance). Este proceso se inicia estableciendo políticas de autenticación utilizando estándares como Sender Policy Framework (SPF) y DomainKeys Identified Mail (DKIM). Se configura registros SPF para especificar los servidores autorizados para enviar correos en nombre del dominio y se genera claves DKIM para firmar digitalmente los correos electrónicos, garantizando su integridad durante el transporte. Además, para completar la implementación de DMARC, se establece un registro DMARC en el DNS del dominio, definiendo políticas de acción para correos electrónicos no autenticados y configurando informes para monitoreo continuo.

9.6 Bloquear tipos de archivos innecesarios

Esta estrategia involucra la configuración de filtros y restricciones específicas en el servidor de correo electrónico mediante el uso de herramientas como Postfix. Se establecieron reglas en los archivos de configuración para restringir la aceptación de archivos potencialmente riesgosos, tales como ejecutables, mediante la definición de patrones de bloqueo. Además, se incorporó la funcionalidad de escaneo de archivos mediante ClamAV para detectar posibles amenazas de malware en los archivos adjuntos.

9.7 Implementar y mantener protecciones antimalware del servidor de correo electrónico

En la implementación de medidas antimalware en mi servidor de correo electrónico, se adoptó una estrategia integral. Primero, instalar y configurar ClamAV para realizar escaneo de archivos adjuntos, asegurándome de actualizar regularmente las definiciones de virus. Luego, integrar ClamAV con mi servidor de correo, en este caso, Postfix, para habilitar el escaneo en la recepción de mensajes. Además, se estable una zona de pruebas para archivos sospechosos, limitando su acceso y configurando políticas específicas para su gestión. Este enfoque no solo fortalece la protección contra amenazas de malware en los correos electrónicos, sino que también proporciona un mecanismo seguro para analizar y gestionar archivos potencialmente riesgosos en

un entorno controlado. Mantengo un monitoreo constante y realizo actualizaciones periódicas para garantizar la efectividad y la seguridad continua del sistema.

Referencias

Firewalld. (2023). *Firewalld.* Obtenido de https://firewalld.org/

Mafla, F. S. (01 de 04 de 2024). *Postgrado UTN.*

26/02/2024

Gerente de Sistemas

Edison Sánchez