UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TITULO DEL TRABAJO DE TITULACIÓN

MONITOREO DE VULNERABILIDADES A LA INFRAESTRUCTURA DE RED DEL DISTRITO DE SALUD

AUTOR

Barrera Cruz, Michaell Jairo

TRABAJO DE TITULACIÓN

Previo a la obtención del grado académico en
MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Amón Salinas, Juan Pablo Mgtr.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
ALICIA GERMANIA ANDRADE VERA

Ing. Alicia Andrade Vera, Mgtr.
COORDINADORA DEL PROGRAMA

Firmado electrónicamente por:
JUAN PABLO AMON SALINAS

Ing. Juan P. Amón Salinas, Mgtr.
TUTOR

SHENDRY BALMORE ROSERO VASQUEZ

Firmado digitalmente porSHENDRY BALMORE ROSERO VASQUEZ
DN: c=SHENDRY BALMORE ROSERO VASQUEZ gn=SHENDRY BALMORE c=EC
Motivo:Soy el autor de este documento
Ubicación:
Fecha:2024-05-14 16:35-05:00

Ing. Shendry Rosero Vásquez, Mgtr.
DOCENTE ESPECIALISTA 1

Firmado electrónicamente por:
DELIA ISABEL CARRION LEON

Ing. Delia Carrión León, Mgtr.
DOCENTE ESPECIALISTA 2

Firmado electrónicamente por:
MARIA MARGARITA RIVERA GONZALEZ

Abg. María Rivera, Mgtr.
SECRETARIA GENERAL UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por Michaell Jairo Barrera Cruz, como requerimiento para la obtención del título de Magister en Tecnologías de la Información.

TUTOR

Firmado electrónicamente por:
JUAN PABLO AMON SALINAS

Ing. Juan Pablo Amón Salinas, Mgtr.

20 días del mes de marzo del año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **MICHAELL JAIRO BARRERA CRUZ**

DECLARO QUE:

El trabajo de Titulación, **MONITOREO DE VULNERABILIDADES A LA INFRAESTRUCTURA DE RED DEL DISTRITO DE SALUD**, previo a la obtención del título en Magister en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Santa Elena, a los 20 días del mes de marzo del año 2024

EL AUTOR

Firmado electrónicamente por:
MICHAELL JAIRO
BARRERA CRUZ

Michaell Jairo Barrera Cruz

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS DE LA INGENIERÍA
INSTITUTO DE POSTGRADO

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **MONITOREO DE VULNERABILIDADES A LA INFRAESTRUCTURA DE RED DEL DISTRITO DE SALUD**, presentado por el estudiante, MICHAELL JAIRO BARRERA CRUZ fue enviado al Sistema Antiplagio COMPILATIO, presentando un porcentaje de similitud correspondiente al **7**%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

TUTOR

Firmado electrónicamente por:
JUAN PABLO AMON SALINAS

Ing. Juan Pablo Amón Salinas, Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
INSTITUTO DE POSTGRADO

AUTORIZACIÓN

Yo, **MICHAELL JAIRO BARRERA CRUZ**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 20 días del mes de marzo del año 2024

EL AUTOR

Firmado electrónicamente por:
MICHAELL JAIRO
BARRERA CRUZ

Michaell Jairo Barrera Cruz

AGRADECIMIENTO

Es imprescindible dar gracias a Dios en primer lugar por la oportunidad que me ha brindado al permitirme ser parte de este proceso de maestría, a mi familia y de forma especial a mi querida esposa Paola, a mis hijos, quienes siempre me brindaron su incondicional apoyo para no desfallecer y poder culminar con éxito este reto, gracias infinitas a mis amigos, compañeros de trabajo y de aulas, que en su momento oportuno también me brindaron la ayuda cuando más necesitaba. A mi tutor de tesis, y a un buen amigo que hice en esta carrera corta, A todos mil gracias.

Michaell Jairo, Barrera Cruz

DEDICATORIA

A Dios por qué es y será mi motor espiritual y al que siempre será el primero a quien debo dedicar todos mis trabajos y proyectos, a Paolita mi esposa que es mi compañera de vida, a mis hijos Jeremías y Julián que son mi motor que me impulsan a seguir en cada proyecto que inicio y que con su paciencia me permiten cristalizarlos, como es esta etapa que estoy finalizando.

Michaell Jairo, Barrera Cruz

ÍNDICE GENERAL

TITULO DEL TRABAJO DE TITULACIÓN I

TRIBUNAL DE SUSTENTACIÓN II

CERTIFICACIÓN III

DECLARACIÓN DE RESPONSABILIDAD IV

CERTIFICACIÓN DE ANTIPLAGIO V

AUTORIZACIÓN VI

AGRADECIMIENTO VII

DEDICATORIA VIII

ÍNDICE GENERAL IX

ÍNDICE DE TABLAS XII

ÍNDICE DE FIGURAS XIII

RESUMEN XIV

ABSTRACT XV

INTRODUCCIÓN 2

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL 7

1.1. Revisión de literatura 7

1.2. Desarrollo teórico y conceptual. 11

1.2.1. Seguridad de la Red 12

1.2.2. Firewalls 12

1.2.3. Cifrado de Datos 12

1.2.4. Autenticación 12

1.2.5. Vulnerabilidades 12

1.2.6. Amenazas Cibernéticas 12

1.2.7. Ransomware: 13
1.2.8. Ataques de Denegación de Servicio (DoS) 13
1.2.9. Phishing 13
1.2.10. El escaneo de vulnerabilidades 13
1.2.11. Herramientas y Tecnologías para el Análisis de Vulnerabilidades 14
1.2.12. Nessus 14
1.2.13. OpenVAS 14
1.2.14. ISO 27001 14
CAPÍTULO 2. METODOLOGÍA 15
2.1. Contexto de la investigación 15
2.2. Diseño y alcance de la investigación 15
2.3. Tipo y métodos de investigación 16
2.4. Población y muestra 16
2.5. Técnicas e instrumentos de recolección de datos 17
2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información. 18
CAPÍTULO 3. RESULTADOS Y DISCUSIÓN 19
3.1 Estado actual de la Infraestructura 19
3.1.1 Características de la Infraestructura 20
3.1.2 Equipos de Comunicación 20
3.1.3 Sistema operativo, servidor proxy, sistemas. 22
3.1.4 Equipo servidor sistema sais 22
3.2 Escaneo de Vulnerabilidades 23
3.2.1 Detalle de vulnerabilidades en la infraestructura de red 29
3.2.2 Análisis de puertos comprometidos 39
3.2.3 Análisis de Vulnerabilidades Con Nmap. 43
3.2.4 Análisis de Vulnerabilidades en el área física donde se encuentra el servidor 44

3.3 Diseño de Plan de Seguridad basados en norma ISO 27001.....45
3.3.1 Esquema de Seguridad.....48
3.3.2 Plan de mejora.....48
3.3.4 Guía para la implementación de controles de seguridad de la información:..51
CONCLUSIONES..... 71
RECOMENDACIONES..... 72
REFERENCIAS..... 73
ANEXOS..... 76

ÍNDICE DE TABLAS

Tabla 1 Ficha técnica de características técnicas de equipo servidor - proxy 20

Tabla 2 Ficha técnica de equipos de comunicación 20

Tabla 3 Ficha técnica de sistemas implementados.....22

Tabla 4 Ficha técnica de equipo sais 23

Tabla 5 Matriz de Vulnerabilidades encontradas.....29

Tabla 6 Niveles de riesgo.....40

Tabla 7 Puertos abiertos analizados con Nmap 43

Tabla 8 Análisis de Vulnerabilidad a la seguridad Física.....44

Tabla 9 Solución a Vulnerabilidades encontradas 46

Tabla 10 Proceso Gestión de Riesgo de Seguridad de la Información.....49

Tabla 11 Políticas de seguridad.....52

Tabla 12 Grupos de interés especial.....53

Tabla 13 Inventario de información y otros activos.....54

Tabla 14 Formación en seguridad de la información 56

Tabla 15 Trabajo a distancia 57

Tabla 16 Perímetro de Seguridad Físicos 59

Tabla 17 Monitoreo de Seguridad Físicos 60

Tabla 18 Servicios de Soporte 61

Tabla 19 Seguridad del Cableado.....62

Tabla 20 Controles a dispositivo de usuario Final 64

Tabla 21 Seguridad de Redes.....66

Tabla 22 Seguridad de los Servicios de Red.....67

Tabla 23 Separación en las Redes 68

ÍNDICE DE FIGURAS

Figura 1 Ubicación geográfica Distrito Salud 15

Figura 2 Diagrama de Red.....19

Figura 3 Configuración de Iptables.....21

Figura 4 Reporte General de primer escaneo.....23

Figura 5 Reporte de vulnerabilidades del primer escaneo.....24

Figura 6 Algoritmos KEX weak.....26

Figura 7 Reporte General de segundo escaneo 28

Figura 8 Detalle de vulnerabilidades segundo escaneo.....28

Figura 9 Resultados de escaneo de puertos 39

Figura 10 Reporte de puertos vulnerables 39

Figura 11 Resultado de escaneos 40

Figura 12 Resultado de Vulnerabilidades por clases de Riesgo 41

Figura 13 Total de Escaneos.....41

Figura 14 Resultado de Vulnerabilidades por CVSS.....42

Figura 15 Total de Escaneos elaborados 42

Figura 16 Resultado de Escaneo con NMAP 43

Figura 17 Estructura PDCA-ISO 27001.....48

RESUMEN

El presente proyecto de investigación tecnológica avanzada tiene como tema principal el Monitoreo de Vulnerabilidades a la infraestructura de red del Distrito Salud, el mismo que tiene como objetivo general Implementar medidas preventivas y de protección para mitigar las vulnerabilidades y fortalecer la seguridad de la infraestructura de red de la entidad administrativa de Salud basado en la norma ISO 27001:2022 y el EGSI. La metodología utilizada en el trabajo investigativo se basa en un diseño no experimental y su alcance de orden explicativo. Mediante un enfoque cualitativo se logró recopilar datos sobre las diferentes amenazas identificadas por lo que se obtuvo una mejor comprensión de percepciones y recomendaciones de los involucrados sobre el tema de seguridad. El método de investigación inductivo se utilizó para observar las incidencias, patrones de vulnerabilidad y posterior obtener conclusiones para un adecuado plan de seguridad de información. A partir del análisis obtenido, se propuso diseñar un plan de mejora normado por el esquema de seguridad para instituciones públicas y su posterior implementación, el mismo que ayudará al proceso de mejora continua de su infraestructura de red de la entidad de salud.

Palabras claves: seguridad de la información, normas ISO 27001, vulnerabilidades

ABSTRACT

The present research project on advanced technological research focuses on Vulnerability Monitoring of the network infrastructure of the Health District. Its main objective is to implement preventive measures and protection to mitigate vulnerabilities and strengthen the security of the network infrastructure of the health administrative entity based on ISO 27001:2022 and EGSI standards. The methodology used in the research work is based on a non-experimental design with an explanatory scope Through a qualitative approach, data was collected on the different threats identified, thereby obtaining a better understanding of the perceptions and recommendations of those involved on the issue of security. An inductive research method was used to observe incidents, vulnerability patterns, and subsequently draw conclusions for an adequate information security plan. Based on the analysis obtained, it was proposed to design an improvement plan standardized by the security scheme for public institutions and its subsequent implementation, which will contribute to the continuous improvement process of the health entity's network infrastructure

Keywords: Information security, ISO 27001 standards, vulnerabilities

INTRODUCCIÓN

De acuerdo a Pérez (2019) son aspectos importantísimos para las entidades: su información y todos los procesos que se lleven a cabo en sus sistemas y redes, por lo que requieren ser protegidos frente a riesgos y amenazas que afecten los 4 principios fundamentales de la seguridad informática, siendo éstos, según Briceño (2021), la disponibilidad, confidencialidad, integridad y autenticación de la información, aspectos vitales para lograr los objetivos que las organizaciones poseen, es así como surge la idea de salvaguardar dichos datos (Muñoz-Zambrano & Zambrano-Rendón, 2023). Por lo que es preciso realizar un análisis de vulnerabilidades o hacking ético que permita realizar una serie de pruebas acordadas con el cliente con el fin de encontrar brechas o fallos de seguridad que pueda afectar el desempeño y producción de la empresa. (Narvaez Narvaez, 2019).

De acuerdo con el trabajo de investigación realizado por Muñoz & Zambrano, el cual señala que, para evaluar las amenazas potenciales según su nivel de riesgo, se deben establecer procedimientos que ejerzan la implementación de controles en función de las políticas y procedimientos, de modo que sirvan como respuesta a incidentes, incluyendo la identificación, mitigación y recuperación. En definitiva, la ciberseguridad como modelo de gestión es un enfoque estratégico que protegerá la información y los activos digitales de una entidad, colaborando con la mejora continua, y promoviendo una cultura de seguridad en toda la organización.(Muñoz-Zambrano & Zambrano-Rendón, 2023).

En su investigación Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study, Fernando Avila señala que implementar adecuadas políticas de ciberseguridad permiten asegurar el funcionamiento de los equipos de comunicación de red en una infraestructura tecnológica hospitalaria, ya que los administradores pueden implementar mecanismos de mitigación a ataques y vulnerabilidades, evitando afectar el funcionamiento de estos dispositivos.(Fernando Avila Pesantez, 2022).

Como objetivo principal del presente trabajo de investigación es el de Implementar medidas preventivas y de protección para mitigar las vulnerabilidades, para fortalecer la seguridad de la infraestructura de red del Distrito de Salud, obteniendo como beneficio la disponibilidad de la información y la seguridad de esta, como se puede denotar el proyecto está orientado a realizar el análisis de las vulnerabilidades que se encuentren en la infraestructura de red y posterior a brindar mejores prácticas de seguridad.

Adicional, una vez realizado el proyecto se busca que otras entidades de salud emulen las buenas prácticas producto del trabajo de investigación de tal forma que también puedan fortalecer su contingente informático a través de nuevos análisis, y de implementaciones, así como el de mejorar su estado actual de seguridad.

Situación de la problemática:

Los ataques cibernéticos se clasificaron como el quinto riesgo más alto en 2021 y se convirtieron en el nuevo estándar para los sectores público, así como para el privado. Esta industria de alto riesgo continuó creciendo en 2022, y se espera que los ataques cibernéticos se dupliquen para 2025, además según lo indica el Informe de Riesgos Globales 2022 del Foro Económico Mundial, en diciembre de 2021, se descubrió una falla critica de seguridad en un software muy utilizado (OMS, 2021). Por otro lado, en su trabajo investigativo Las oportunidades de crecimiento de la ciberseguridad de la salud de EE. UU, Sulivan indica que existieron datos donde reflejaban que más de 100 intentos de explotar la vulnerabilidad fueron detectados cada minuto y más del 90 por ciento de todas las organizaciones de salud han reportado al menos una brecha de ciberseguridad en los últimos tres años. (Sulivan, 2023).

La infraestructura de red desempeña un papel fundamental en el funcionamiento eficiente de diversas organizaciones y sectores. En este contexto, el área de la salud enmarcado en la atención médica, la disponibilidad y seguridad de la información son

esenciales para proporcionar servicios médicos de calidad y salvaguardar los datos sensibles de los pacientes. Para el caso de las entidades estatales en el Ecuador, las mismas que proporcionan los servicios en salud, los equipos pertenecientes a la infraestructura de red cobran una importancia notable para mantener la comunicación en toda la red, puesto que permite la transmisión, recepción y conservan la disponibilidad de la información en línea. Como señala Fernando Avila, con el pasar del tiempo los atacantes informáticos han descubierto nuevos métodos para ganar dinero y la industria de la salud se está convirtiendo en un objetivo fácil, debido a la capacidad de vender grandes lotes de datos personales con fines de lucro.(Fernando Ávila Pesantez et al., 2022)

El Distrito de Salud, como entidad encargada de brindar servicios de salud, en la provincia de Santa Elena a través de sus 24 unidades operativas y 1 Hospital Básico, se enfrenta a desafíos y preocupaciones relacionadas con la gestión y supervisión de su infraestructura de red, dado que mantiene sus plataformas con libre acceso sin tener muy en cuenta la seguridad.

Planteamiento de la investigación

Hoy en día la infraestructura de red se ha convertido en el pilar fundamental para el funcionamiento eficiente de organizaciones de todos los sectores.

(Mayorga, 2018) En su estudio nos recalca que, en el ámbito internacional, los Estados conscientes de los problemas que traen consigo el avance de la tecnología y las comunicaciones, están prestando más atención a sus sistemas de ciberseguridad y ciberdefensa. Aunque también es cierto, que aún son muchos los países que no han analizado las consecuencias potenciales de un posible ataque cibernético, y ni si quiera se están preparando para ello.

Hoy en día, las organizaciones hacen todo lo posible para mantener el control y ayudar a proteger sus redes corporativas y su activo de información de las amenazas cibernéticas, es por ello que se hace necesario garantizar la seguridad de los datos mientras viaja por la red pública.(Carrión-Barco et al., 2021, p. 2)

El Distrito de Salud, como entidad encargada de proporcionar servicios de salud en el cantón Santa Elena, se enfrenta al desafío en cuanto a la gestión y operación de su infraestructura de red, esto debido a las innumerables ocasiones en que la parte presupuestaria merma la factibilidad de implementar mecanismos de mitigación y protección de datos. Y si a esto adicionamos que dentro de esta misma infraestructura se debe mantener una correcta interconexión de dispositivos médicos, el acceso a historias clínicas electrónicas, la comunicación interna y externa, así como la seguridad de los datos de los pacientes, son aspectos críticos que dependen de una infraestructura de red sólida y confiable.

La justificación de este estudio radica en la necesidad de implementar un mecanismo de monitoreo de la infraestructura de red en el Distrito de Salud desarrollado mediante herramientas open source, de esta forma se podrá efectuar el plan de seguridad no solo para la información sino también de la red, ayudará a mitigar posibles interrupciones en los servicios médicos, y enmascarar la exposición a vulnerabilidades de seguridad.

Formulación del problema de investigación

Para el desarrollo de objetivos se plantearon los siguientes cuestionamientos:

General:

- *¿Cómo se puede detectar de manera temprana fallas, optimizar el rendimiento y salvaguardar la seguridad de la información en la infraestructura de red de Distrito de Salud?*

Específicos*:*

- *¿Cuál es el estado actual de las medidas de seguridad de la información en la entidad de Salud?*
- *¿Cuáles son las principales vulnerabilidades que afectan actualmente la infraestructura de red en el Distrito de Salud?*
- *¿De qué manera se podría garantizar que se lleven a cabo las prácticas adecuadas de seguridad?*

Objetivo General:

Implementar medidas preventivas y de protección para mitigar las vulnerabilidades y fortalecer la seguridad de la infraestructura de red del Distrito de Salud.

Objetivos Específicos:

1. Determinar la situación actual de la seguridad a la infraestructura tecnológica en la entidad de Salud.
2. Definir las vulnerabilidades de la infraestructura de red del Distrito de Salud para establecer recomendaciones para el mejoramiento de seguridad de información basados en la norma ISO 27001.
3. Desarrollar un plan de seguridad de información destacando las mejores prácticas basados en la norma ISO 27001.

Planteamiento hipotético

Dentro del trabajo en desarrollo podemos plantear la siguiente hipótesis:

Hipótesis: *Implementar medidas preventivas y de protección a la infraestructura de red del Distrito de Salud conducirá a una mejora significativa en la identificación temprana y mitigación de vulnerabilidades de tal forma que permita fortalecer la seguridad en la red.*

Esta hipótesis propone realizar un análisis de vulnerabilidades en la infraestructura de red del Distrito de Salud el mismo que tendrá un impacto positivo en la seguridad y el rendimiento de la red, lo que permitirá implementar medidas preventivas y brindar una mejor protección de la información y una prestación más eficaz de los servicios de salud.

CAPÍTULO 1. MARCO TEÓRICO REFERENCIAL

En este apartado se explora con bases teóricas, conceptualizaciones y proyectos materia de ejemplo que ayudará a comprender de mejor manera la propuesta de investigación tecnológica, considerando en este caso la importancia relevante de implementar las mejores prácticas y planes de seguridad de la información, mediante análisis de vulnerabilidades en una entidad de Salud.

1.1.Revisión de literatura

Dentro del marco teórico referencial se aborda la teoría necesaria para brindar las bases que permitan alcanzar el entendimiento del proyecto como tal, definiendo los siguientes referencias:

En su trabajo Caso De Estudio Para El Análisis De Vulnerabilidad Y Propuesta De Aseguramiento De La Seguridad De La Información En La Infraestructura Tecnológica De La Empresa Nostradamus S.a.S, Mejía señala como objetivo principal el analizar desde un enfoque técnico los ataques a los sistemas de información registrados en el caso de estudio, con el fin de plantear, desde un enfoque administrativo, un proyecto de diseño para la posterior implementación de un sistema de gestión para la seguridad de la información, basado en la norma ISO 27001, con el fin de reforzar el aseguramiento de la información en la infraestructura tecnológica de la empresa; esto denota claramente la importancia sobremanera de realizar los correspondientes análisis de vulnerabilidades para obtener al final las mejoras necesarias.(Mejía, 2020).

Por su parte *(Liliana Parra, 2017)* en su investigación*: Análisis de vulnerabilidades en la infraestructura tecnológica de una empresa, utilizando herramientas de Test de Intrusión;* nos indica que su trabajo toma la relevancia adecuada sobre como incide el no contar con un monitoreo de seguridad, no solo para empresas sino para toda entidad, adicional que el proyecto tiene como objetivo el analizar las vulnerabilidades presentes en la red de la empresa, utilizando estándar OSSTM para evitar acceso no autorizado a los procesos del sistema de información, de tal forma que

al final se elabore un informe de auditoría de seguridad informática detallando los hallazgos de la red del Instituto.

Por otro lado en la investigación Seguridad Ofensiva Mediante Hacking Ético para Fortalecer Infraestructuras en Redes de Telecomunicación, Cuadros Navarro nos menciona en su trabajo Seguridad Ofensiva Mediante Hacking Ético para Fortalecer Infraestructuras en Redes de Telecomunicaciones, como generar un plan de aseguramiento de la información, aplicando normas destinadas a cumplir con este objetivo, como es el caso de la ISO 27001 y usando la metodología de Seguridad Ofensiva; para este propósito, se estableció un esquema controlado para la realización de una auditoria de seguridad informática mediante pruebas de penetración utilizando técnicas de hacking ético a infraestructuras de redes de telecomunicaciones, con el objetivo de detectar las vulnerabilidades para poder determinar con efectividad las medidas necesarias a tomar.(Cuadros Navarro et al., 2022)

Mientras que en la investigación *Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study*; Avila define que las políticas de ciberseguridad permiten asegurar el funcionamiento de los equipos de comunicación de red en una infraestructura tecnológica hospitalaria, ya que los administradores pueden implementar mecanismos de mitigación a ataques y vulnerabilidades, evitando afectar el funcionamiento de los equipos, a su vez este trabajo se tomó como referencia la norma ISO 27032 para seguir los lineamientos de cuatro fases: entendimiento de la organización, análisis de riegos, plan de acciones e implementación, que permitieron proponer las políticas de ciberseguridad necesarias para la infraestructura de red en equipos de marca Huawei; adicional en la primera etapa se realizaron pruebas de vulnerabilidades con las herramientas OPENVAS y Yersinia, estableciendo la probabilidad de ataques tales como MAC-ARP, DHCP Starvation, ataque STP, Vlan hopping, entre otros; y mediante las respectivas configuraciones y habilitación de funcionalidades, se pudo mitigar una cantidad significativa del 98% de las vulnerabilidades existentes en el estado inicial de la infraestructura de red hospitalaria.(Fernando Avila Pesantez et al., 2022).

(Ortiz-Lazo & Vizñay-Duran, 2019). Por su parte con su investigación: *Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel*; se refiere a la presentación de un análisis de riesgos y vulnerabilidades de la información, utilizando la norma ISO 27005:2008 en donde nos permite identificar, analizar, evaluar los diferentes tipos de riesgo que se tiene en una organización, permitiendo establecer controles o salvaguardias con la finalidad de mitigar el riesgo. Los resultados de este trabajo aportan a la alta gerencia en la toma de decisiones, para el tratamiento del riesgo mediante normas, estándares y buenas prácticas, sin afectar la información de la empresa y tener continuidad en el negocio y alcanzar los objetivos planteados por la organización.

(Gilces Zambrano et al., 2021) Nos refiere en su investigación: Mecanismos de ciberseguridad basados en honeypots, que la evolución vertiginosa de las tecnologías de la información y comunicación, ha generado en la sociedad contemporánea una creciente necesidad de interacción entre medios digitales y la mayoría de nuestras actividades productivas; sin embargo, a la par del auge de mayores y mejores oportunidades que nacen de esta sinergia, han ido apareciendo nuevos tipos de riesgos y amenazas computacionales, que han convertido a la seguridad de las redes en un problema de proporciones masivas; bajo este contexto, es necesario prestar mayor atención en el estudio de soluciones que permitan asegurar las disponibilidad de las comunicaciones

Avila por su parte en el trabajo de investigación Ransomware, una amenaza latente en Latinoamérica, señala que las políticas de ciberseguridad permiten asegurar el funcionamiento de los equipos de comunicación de red en una infraestructura tecnológica hospitalaria, ya que los administradores pueden implementar mecanismos de mitigación a ataques y vulnerabilidades, evitando afectar el funcionamiento sus equipos; donde los administradores de red implementan seguridades tanto en software como en hardware, dando relevancia a las capas superiores del modelo OSI; sin embargo, se relegan las capas inferiores que son infraestructuras más vulnerables y según el reporte del FBI, el 80% de los ataques a la capa de red provienen del interior de la entidad, debido a que el 99% de

los puertos de los equipos de conexión están sin restricciones, de tal forma que cualquier usuario pueda conectarse a ellos (Fernando Ávila Pesantez et al., 2022).

Por otro lado en su trabajo de titulación *Implementación de un plan de seguridad informática con la norma ISO/IEC 27001 en la empresa Ransa comercial*, Vladimir señala que "la problemática de la empresa surge porque ejecuta todos sus procesos en Excel y no lleva un control de todos sus procesos, lo que significa que su información este expuesta a diferentes ataques cibernéticos y posibles pérdidas de información, la investigación tuvo como objetivo general implementar un plan de seguridad informática utilizando la norma ISO/IEC 27001 en la empresa Ransa Comercial S.A – Piura; 2021, para mejorar la seguridad de información de sus clientes. El tipo de la investigación es cuantitativo, el nivel de investigación es descriptivo y el diseño de la investigación es no experimental y de corte transversal. Los resultados de la dimensión 01: Nivel de satisfacción con el sistema actual; el 60.00% de los trabajadores encuestados NO están satisfechos con el sistema actual, mientras que el 40.00% indicaron que SI, en relación a la segunda dimensión, se observó que el 80.00% de los encuestados sostienen que SI creen necesario de una nueva propuesta, mientras que el 20% indicaron que NO, esta investigación tiene como alcance resguardar la confidencialidad de los activos de información en la empresa, por lo que se concluyó que la implementación de un plan de seguridad informática en la empresa Ransa Comercial S.A, mejoró la seguridad de información de sus clientes"(Dr. Vladimir, 2021).

En su trabajo Seguridad Ofensiva Mediante Hacking Ético para Fortalecer Infraestructuras en Redes de Telecomunicaciones, Cuadros indica que con el crecimiento exponencial del uso del internet y debido a la alta incidencia de ataques cibernéticos destinados a encontrar vulnerabilidades en los servicios de redes y comunicación; en los últimos años se ha incrementado la adopción de medidas de seguridad en las direcciones de Tecnologías de Información y Comunicación (TIC) de las instituciones públicas. El objetivo de la presente investigación es generar un plan de aseguramiento de la información, aplicando normas destinadas a cumplir con este objetivo, como es el caso de la ISO 27001 y usando la metodología de Seguridad Ofensiva (OS). Para este

propósito, se estableció un esquema controlado para la realización de una auditoria de seguridad informática mediante pruebas de penetración utilizando técnicas de hacking ético a infraestructuras de redes de telecomunicaciones, con el objetivo de detectar las vulnerabilidades para poder determinar con efectividad las medidas necesarias a tomar.(Cuadros Navarro et al., 2022).

En el trabajo Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa Cybersecurity de Colombia ITDA, Ramírez nos señala que, teniendo como referencia la norma ISO 27001 se deberán implementar las políticas de seguridad y un plan de continuidad de negocio; donde se realizarán análisis de los diferentes riesgos que existen de acuerdo a los diferentes activos con los que las organizaciones cuenten y dependiendo de este análisis se procede a implementar los mecanismos necesarios para minimizarlos y que los activos funcionen perfectamente y ayuden a cumplir con las metas y objetivos de las entidades, esto servirá como base para poder implementar un plan de políticas de seguridad basados en la norma.(Ramírez, 2020)

1.2.Desarrollo teórico y conceptual.

Este apartado ayudará a comprender la terminología que se utilizará en el desarrollo del proyecto.

(Flores Robaina et al., 2021), en su artículo menciona que “El empleo de las tecnologías de la información y la comunicación en el sector de la salud mejoran considerablemente el funcionamiento de los procesos asistenciales y de gestión médico-administrativa, todo lo cual contribuye a una mayor eficiencia hospitalaria y desempeño competitivo de las instituciones”

(Martin, 2022) en su trabajo de investigación acota que “El uso generalizado de dispositivos inteligentes y las numerosas debilidades de seguridad de las redes han aumentado drásticamente el número de ciberataques en el Internet de las cosas (IOT)”

1.2.1. Seguridad de la Red

La seguridad de red es cualquier actividad diseñada para proteger el acceso, el uso y la integridad de la red y los datos corporativos. Incluye tecnologías de hardware y software. Está orientada a diversas amenazas. Evita que ingresen o se propaguen por la red. La seguridad de red eficaz administra el acceso a la red. (Cisco, 2023). Esto implica garantizar que la red no sea vulnerable a amenazas y ataques cibernéticos que puedan comprometer la privacidad de la información, la integridad de los datos y la continuidad de los servicios. Algunos aspectos clave de la seguridad de la red incluyen

1.2.2. Firewalls

Dispositivo de seguridad de la red que monitorea el tráfico entrante y saliente y a su vez decide si permite o bloquea este mismo tráfico en función de un conjunto definido de reglas de seguridad. (CISCO, 2023).

1.2.3. Cifrado de Datos

El cifrado en ciberseguridad es la conversión de datos de un formato legible a un formato codificado. (Paredes, 2022)**.**

1.2.4. Autenticación

Verificación de la identidad de un usuario o dispositivo antes de permitir el acceso a la red. La autenticación es el proceso de confirmar la autenticidad de un cliente para identificar su validez. Si el usuario es válido, el servidor permite la accesibilidad de sus activos (Prakash & Kumar, 2018)

1.2.5. Vulnerabilidades

(Guevara-Vega E, Delgado-Deza J, Mendoza-de-los-Santos A Revista Científica de Sistemas e Informática (2023) mencionan que las vulnerabilidades vienen a ser la inconsistencia de los sistemas, donde éstas pueden servir para un cibercriminal o atacante con la intención de afectar negativamente los activos de información.

1.2.6. Amenazas Cibernéticas

Las amenazas cibernéticas son acciones maliciosas realizadas por individuos, grupos o programas informáticos diseñados para comprometer la seguridad de la red o del sistema. En el estudio Experiencias de seguridad cibernética en países europeos y latinoamericanos, Otilia menciona que las ciberamenazas se hacen pasar por organismos

oficiales e institucionales y de esa manera poder obtener la información personal o de las redes corporativas y gubernamentales, y esto debido a que las personas están trabajando desde espacios que son poco seguros, lo cual conlleva a la vulnerabilidad de la ciberseguridad de un Estado. (Otilia Mosquera-Chere, 2021).

1.2.7. Ransomware:

Malware bastante interesante que, después de infectar el sistema, bloquea algunos recursos populares e importantes del sistema informático y luego exige dinero de rescate para devolver el acceso. (Ávila Niño, 2023, p. 2)

1.2.8. Ataques de Denegación de Servicio (DoS)

En el estudio de que son los ataques Dos, Kaspersky indica que estos son intentos de sobrecargar un sistema o red con tráfico malicioso para hacer que los servicios sean inaccesibles, adicional están los ataques a la red distribuidos se denominan a menudo ataques de denegación de servicio distribuidos (DDoS). Este tipo de ataque aprovecha los límites de capacidad específicos que se aplican a los recursos de red, como la infraestructura sobre la que se basa el sitio web de una empresa. (Kaspersky Lab, 2021).

1.2.9. Phishing

El phishing es un acto fraudulento en línea que utiliza ingeniería social y recursos técnicos para engañar a los usuarios de Internet y adquirir sus datos sensibles o información crítica en línea (*Gowtham y Krishnamurthi, 2014, Gupta et al., 2016).*

1.2.10. El escaneo de vulnerabilidades

Es una práctica esencial en la seguridad de la infraestructura de red. Esta técnica implica el uso de herramientas de escaneo de vulnerabilidades para identificar activamente debilidades en sistemas, aplicaciones y configuraciones de red. El autor del trabajo de investigación *(Rodríguez, 2018)* en su Diseño de Manual básico de pruebas de hacking ético: Escaneo de red, ilustra a detalle cómo se debe desarrollar el escaneo de vulnerabilidades, los mismos que puedan afectar los equipos que hacen parte de una red. Esto permite analizar los requerimientos que se deben tener en cuenta para aumentar los niveles de seguridad de la red y los equipos conectados. Finalmente, se genera un manual como guía para los administradores de red que pueden aplicar a los servidores.

1.2.11. Herramientas y Tecnologías para el Análisis de Vulnerabilidades

Es necesario saber qué tipo de información se desea recopilar para escoger la herramienta que más se adapte. Ejemplo de aquello es Nessus, el cual, permite el análisis de vulnerabilidades por medio de escaneo múltiple sobre diferentes arquitecturas, los resultados de los análisis son mostrados en un informe de manera detallada. *(Rodríguez, 2018)*

1.2.12. Nessus

El escáner de vulnerabilidades de Nessus es el líder mundial en escáneres activos y ofrece descubrimiento de alta velocidad, auditoría de configuración y elaboración de perfiles de activos, descubrimiento de datos confidenciales y análisis de vulnerabilidades de nuestra postura de seguridad. Nessus tiene la capacidad de descubrir el estado del puerto y también detecta fallas en un sistema particular con una solución recomendada para solucionarlo. *(Ch, 2020)*

1.2.13. OpenVAS

Es un marco de varios servicios y herramientas que ofrece una solución integral y potente de escaneo y gestión de vulnerabilidades. El marco es parte de la solución comercial de gestión de vulnerabilidades de Greenbone Networks desde la cual se aportan desarrollos a la comunidad de código abierto desde 2009. *(Rahalkar, 2019)*.

1.2.14. ISO 27001

Un Sistema de Gestión de Seguridad de la Información, según la Norma UNE-ISO/IEC 27001, es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Esto significa que se va a dejar de operar de una manera intuitiva y se va a empezar a tomar el control sobre lo que sucede en los sistemas de información y sobre la propia información que se maneja en la organización.(Ramírez, 2020).

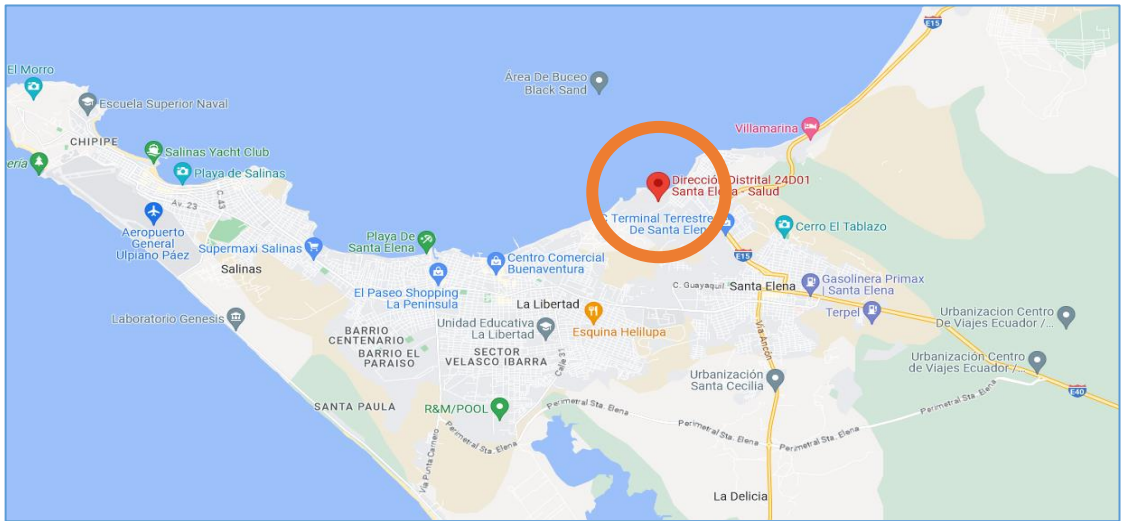
CAPÍTULO 2. METODOLOGÍA

2.1. Contexto de la investigación

El proyecto de investigación ayudará a implementar un plan de seguridad de la información, el mismo que se realizará mediante un previo análisis de vulnerabilidades a la infraestructura de red del Distrito de Salud, localizado en la provincia de Santa Elena, Parroquia Ballenita, Av. Occidental y Calle Patronato, ubicado en las siguientes coordenadas: latitud -2.208455077160473, longitud -80.87704207246671.

Figura 1

Ubicación geográfica Distrito Salud



Nota. tomada de Google Maps

2.2. Diseño y alcance de la investigación

El trabajo de investigación se centra en el análisis de las técnicas y herramientas utilizadas en el monitoreo de vulnerabilidades en una infraestructura de red. El objetivo principal es comprender y proponer soluciones eficaces para identificar y mitigar vulnerabilidades en la infraestructura de red del Distrito de Salud.

El alcance de este proyecto de tesis se concentra en la investigación, análisis y propuesta de soluciones para el monitoreo de vulnerabilidades en una infraestructura de red de una entidad de salud pública, por lo que se considera que la investigación será de ***carácter no experimental***, y su alcance será de orden explicativo.

2.3. Tipo y métodos de investigación

Tipo de Investigación: De acuerdo con la naturaleza del trabajo de investigación el proyecto es considerado como:

1. **Cualitativo:** El objetivo es recopilar datos sobre las amenazas identificadas, tipos de vulnerabilidad, realizar encuestas estructuradas para medir la percepción de seguridad de los usuarios del área de tecnologías, por lo que se podrá obtener una comprensión detallada de las experiencias, percepciones y recomendaciones de los participantes, lo que enriquecerá la investigación y permitirá explorar los temas de manera más holística y contextual.

Método de Investigación:

1. **Inductivo:** Se utilizará este método para observar patrones de vulnerabilidades específicas en la infraestructura de red y luego derivar conclusiones sobre las prácticas de seguridad.

2.4. Población y muestra

Población de Estudio:

La población de estudio es el grupo de interés o conjunto de elementos que están sujetos a investigación. En este caso, la población de estudio podría ser:

- **Personal de TI** en el Distrito de Salud, ya que el objetivo es evaluar la percepción y el conocimiento de la seguridad de la red entre los actores.
- **La infraestructura de red** en el Distrito de Salud para poder evaluar la seguridad de la infraestructura de red como tal.

Muestreo:

Debido a la naturaleza de la población, en este punto no aplica un muestreo como tal**.**

2.5. Técnicas e instrumentos de recolección de datos

- ***Encuesta*:** Para el desarrollo del proyecto de investigación será ideal recopilar datos cualitativos, como por ejemplo las estadísticas sobre la percepción de seguridad de la red, tipos de vulnerabilidad, así como establecer los niveles de conocimiento de seguridad por parte del personal de TI. *(ver anexo 5, pág. 114*)

- Adicional se utilizará el sistema base ***Kali Linux*** en su versión 2023.3, el mismo que servirá para identificar posibles anomalías que puedan indicar actividades maliciosas o vulnerabilidades en la infraestructura de red. Kali Linux también incluye herramientas para la recopilación de datos, como la extracción de información de servidores web, bases de datos y otros sistemas de información que puedan ser relevantes para la investigación. *(Parra Barzola, 2017)* cita en su investigación que las aplicaciones instaladas en el sistema operativo Kali Linux que se utilizarán para el análisis de vulnerabilidades en una infraestructura tecnológica son de código abierto por la cual no se requiere que la institución, entidad o empresa, invierta en software licenciado para ejecutar la respectiva auditoria de seguridad informática.

- **Así como también, se u**tilizarán herramientas adicionales dentro del sistema base tales como Nessus, OpenVAS; que deben ser instaladas y configuradas de manera correcta en la versión de Kali, para realizar escaneos de vulnerabilidades en la infraestructura de red. Estas herramientas permitirán identificar y evaluar las vulnerabilidades en los equipos, sistemas y dispositivos de red.

En el trabajo de investigación se aplicó la encuesta (*Anexo 5*) el mismo que marca un punto de partida para definir el ámbito de análisis propio de la infraestructura, así como la percepción general de la seguridad que existe dentro la misma por parte de los funcionarios de tecnologías.

2.6. Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información**.**

Evaluación de la Validez y Confiabilidad en una Encuesta:

Validez:

2.6.1 Validez**:** Antes de aplicar la encuesta, se debe asegurar de que las preguntas sean relevantes y representativas con relación a lo que se va a medir, y esto se puede lograr mediante revisiones por expertos, especialistas en Seguridad de la Información o Ciberseguridad.

2.6.2 Referencia de uso de herramienta: las herramientas como tal son referenciadas por un experto en materia de Seguridad Informática, el mismo que brindó la asesoría para la elección idónea de la aplicación.

2.6.3 Pruebas piloto con el personal de TI: se realizan pruebas en el campo de la encuesta para validar los cuestionamientos, así como el laboratorio implementado para su ejecución y escaneo de vulnerabilidades.

Confiabilidad de los resultados:

Confiabilidad Test: Administrar la encuesta al grupo de funcionarios de TI en un período de tiempo, razón por la que deberá desarrollar antes de aplicar las mejoras.

Análisis de Consistencia de Respuestas: servirá para poder analizar si las respuestas de los funcionarios de TI son coherentes, de tal forma que, si un funcionario indica que está "muy satisfecho" en una pregunta y "muy insatisfecho" en la siguiente, eso podría indicar un problema de consistencia.

Es importante realizar pruebas de validez y confiabilidad antes de administrar la encuesta. Si se encuentra problemas de validez o confiabilidad, se deberán realizar ajustes en las preguntas o en el diseño de la encuesta según sea necesario.

CAPÍTULO 3. RESULTADOS Y DISCUSIÓN

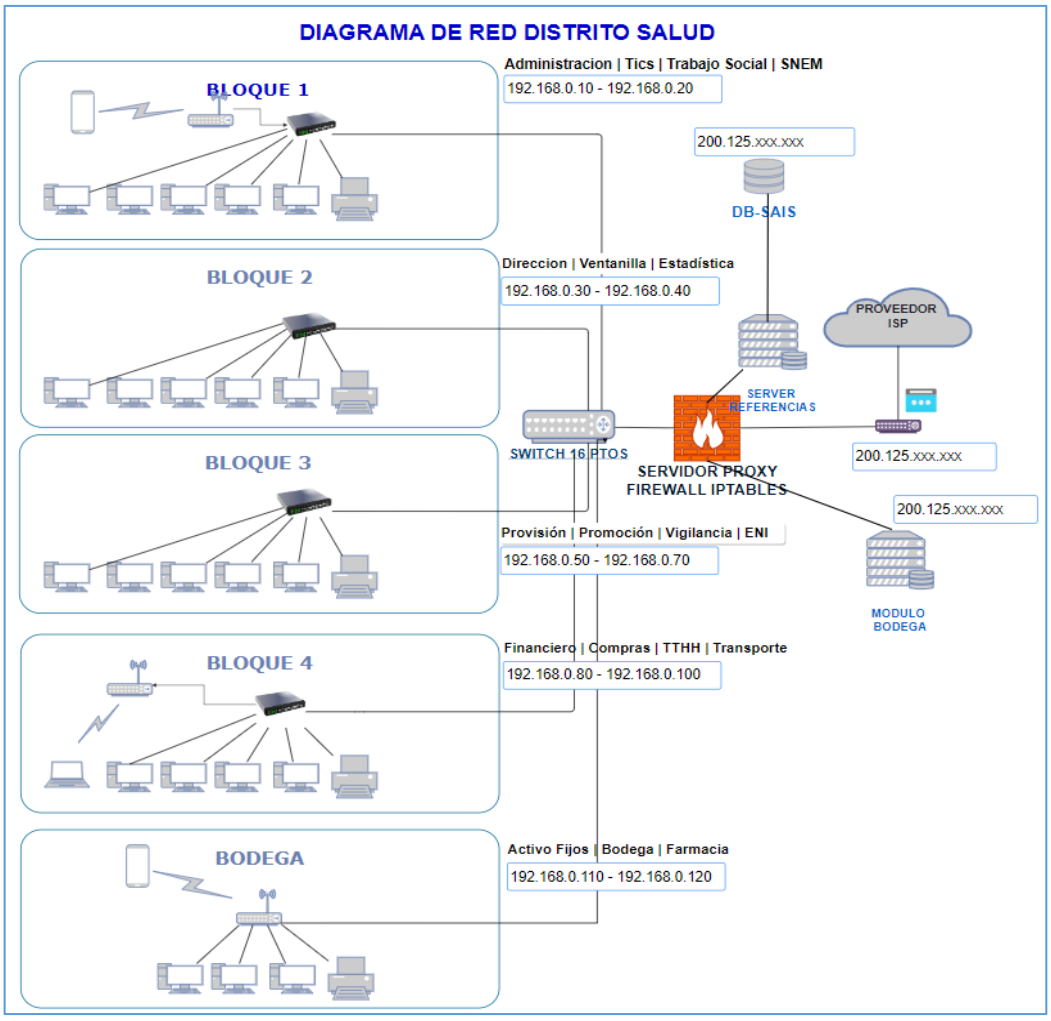
En este apartado se expondrán la situación actual de la infraestructura de red, así como los resultados de los escaneos de vulnerabilidades realizados mediante las herramientas ya probadas en el laboratorio, y desarrollar finalmente un plan de seguridad de información destacando las mejores prácticas.

3.1 Estado actual de la Infraestructura

Para poder determinar la infraestructura objetivo, es necesario definir el diseño real del área, por lo que presento el diagrama de red con los elementos que se detallan a continuación.

Figura 2

Diagrama de Red



Nota. Elaboración propia

3.1.1 Características de la Infraestructura

En este apartado se presenta la ficha técnica del equipo servidor donde se encuentra alojado tanto el servicio proxy como el aplicativo soporte de inventario bodega de la entidad de Salud - Santa Elena.

Tabla 1

Ficha técnica de características técnicas de equipo servidor - proxy

FICHA TÉCNICA DE EQUIPO SERVIDOR	
Tipo Equipo	HP pro6300
Procesador	Intel corei5
Memoria RAM	16GB
Almacenamiento	1 TB
Fuente alimentación	450W
Puerto Red	LAN 10/100/1000

Nota. Características obtenidas desde el servidor Proxy

Se recalca que el equipo detallado en la tabla cubría requerimiento inicial por la demanda propia de las plataformas y con proyección a fututo de las diferentes necesidades, derivando así en el componente físico descrito.

3.1.2 Equipos de Comunicación

Dentro del parque tecnológico de comunicaciones se cuenta con el siguiente equipamiento:

Tabla 2

Ficha técnica de equipos de comunicación

FICHA TÉCNICA DE EQUIPO DE COMUNICACIONES		
CANTIDAD	**EQUIPO**	**CARACTERISTICAS**
5	SWITCH	TPLINK 16 puertos
1	ROUTER	Nexxt ARN-02304U2
1	FIREWALL	Proxy | Iptables*

FICHA TÉCNICA DE EQUIPO DE COMUNICACIONES		
3	ACCES POINT	AP-AC-LR
1	CABLEADO	UTP CAT6

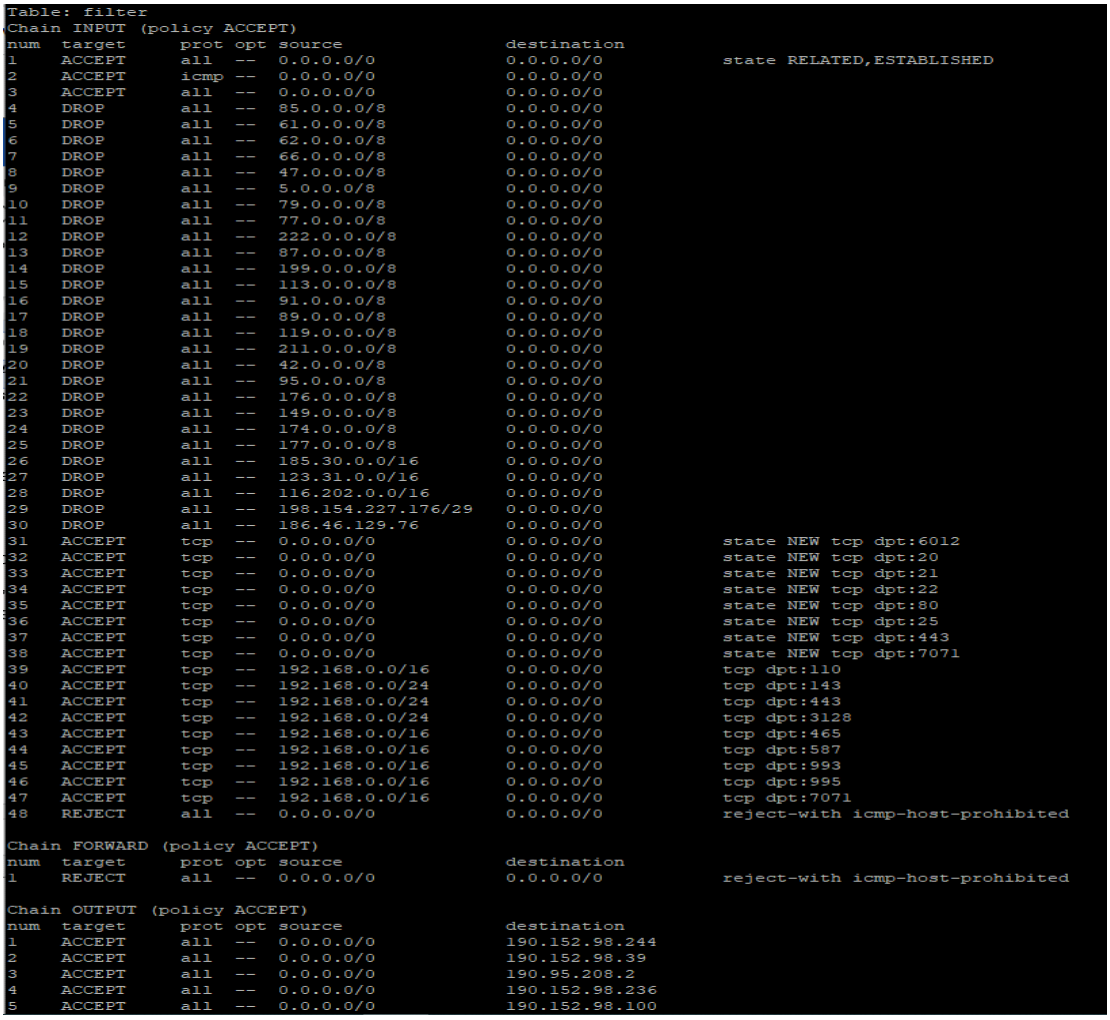
Nota. Equipamiento de Red, elaboración propia

Detalle de Firewall implementado en equipo Proxy mediante reglas de iptables

El equipo servidor mantiene como plataforma base el sistema operativo Linux CentOS en su versión 6.10 i386, conociendo aun de su seguridad como tal, se tiene activado la opción de firewall bajo parámetros configurados en iptables como se detalla a continuación:

Figura 3

Configuración de Iptables



```
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
2    ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0
3    ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
4    DROP       all  --  85.0.0.0/8           0.0.0.0/0
5    DROP       all  --  61.0.0.0/8           0.0.0.0/0
6    DROP       all  --  62.0.0.0/8           0.0.0.0/0
7    DROP       all  --  66.0.0.0/8           0.0.0.0/0
8    DROP       all  --  47.0.0.0/8           0.0.0.0/0
9    DROP       all  --  5.0.0.0/8            0.0.0.0/0
10   DROP       all  --  79.0.0.0/8           0.0.0.0/0
11   DROP       all  --  77.0.0.0/8           0.0.0.0/0
12   DROP       all  --  222.0.0.0/8          0.0.0.0/0
13   DROP       all  --  87.0.0.0/8           0.0.0.0/0
14   DROP       all  --  199.0.0.0/8          0.0.0.0/0
15   DROP       all  --  113.0.0.0/8          0.0.0.0/0
16   DROP       all  --  91.0.0.0/8           0.0.0.0/0
17   DROP       all  --  89.0.0.0/8           0.0.0.0/0
18   DROP       all  --  119.0.0.0/8          0.0.0.0/0
19   DROP       all  --  211.0.0.0/8          0.0.0.0/0
20   DROP       all  --  42.0.0.0/8           0.0.0.0/0
21   DROP       all  --  95.0.0.0/8           0.0.0.0/0
22   DROP       all  --  176.0.0.0/8          0.0.0.0/0
23   DROP       all  --  149.0.0.0/8          0.0.0.0/0
24   DROP       all  --  174.0.0.0/8          0.0.0.0/0
25   DROP       all  --  177.0.0.0/8          0.0.0.0/0
26   DROP       all  --  185.30.0.0/16        0.0.0.0/0
27   DROP       all  --  123.31.0.0/16        0.0.0.0/0
28   DROP       all  --  116.202.0.0/16       0.0.0.0/0
29   DROP       all  --  198.154.227.176/29   0.0.0.0/0
30   DROP       all  --  186.46.129.76        0.0.0.0/0
31   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:6012
32   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:20
33   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:21
34   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:22
35   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:80
36   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:25
37   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:443
38   ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           state NEW tcp dpt:7071
39   ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0           tcp dpt:110
40   ACCEPT     tcp  --  192.168.0.0/24       0.0.0.0/0           tcp dpt:143
41   ACCEPT     tcp  --  192.168.0.0/24       0.0.0.0/0           tcp dpt:443
42   ACCEPT     tcp  --  192.168.0.0/24       0.0.0.0/0           tcp dpt:3128
43   ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0           tcp dpt:465
44   ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0           tcp dpt:587
45   ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0           tcp dpt:993
46   ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0           tcp dpt:995
47   ACCEPT     tcp  --  192.168.0.0/16       0.0.0.0/0           tcp dpt:7071
48   REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    REJECT     all  --  0.0.0.0/0            0.0.0.0/0           reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     all  --  0.0.0.0/0            190.152.98.244
2    ACCEPT     all  --  0.0.0.0/0            190.152.98.39
3    ACCEPT     all  --  0.0.0.0/0            190.95.208.2
4    ACCEPT     all  --  0.0.0.0/0            190.152.98.236
5    ACCEPT     all  --  0.0.0.0/0            190.152.98.100
```

Nota: tomada del archivo iptables del Equipo Servidor proxy firewall

3.1.3 Sistema operativo, servidor proxy, sistemas.

El Sistema operativo base instalado en el equipo servidor ubicado en la Sede de la Dirección Distrital 24D01 Santa Elena es Linux CentOS v. 6.10 con kernel 2.6.32-754.6.3.el6.i686 Gnome 2.28.2

Se describe también la siguiente información sobre las plataformas utilizadas en el lugar objeto de análisis.

Tabla 3

Ficha técnica de sistemas implementados

ITEM	DETALLE
Sistema Inventario 24D01	Módulo que permite gestión de bodega y activos
Sistema de Referencias 24D01	Módulo que permite gestionar las diferentes referencias médicas desde las 24 unidades operativas a los hospitales asignadas a la zona 5.
Web Proxy	Mecanismo utilizado para el filtrado de navegación, y brinde acceso a los diferentes conectados. El firewall es gestionado mediante reglas de iptables configurados en el sistema base CentOS.
SAIS	Sistema de Atención Integral en Salud, el mismo que funciona para registros de atención médica.

Nota. Detalle de los sistemas implementados en los servidores, elaboración propia

3.1.4 Equipo servidor sistema sais

El equipo en mención mantiene almacenada la información de registros médico, que atienden en el hospital, parte de las unidades operativas que administra la entidad de Distrito de Salud

Tabla 4

Ficha técnica de equipo sais

FICHA TÉCNICA DE EQUIPO SAIS	
Tipo Equipo	Dell Optiplex 5000
Procesador	Intel corei7
Memoria RAM	16GB
Almacenamiento	1 TB SSD
Fuente alimentación	450W
Puerto Red	LAN 10/100/1000

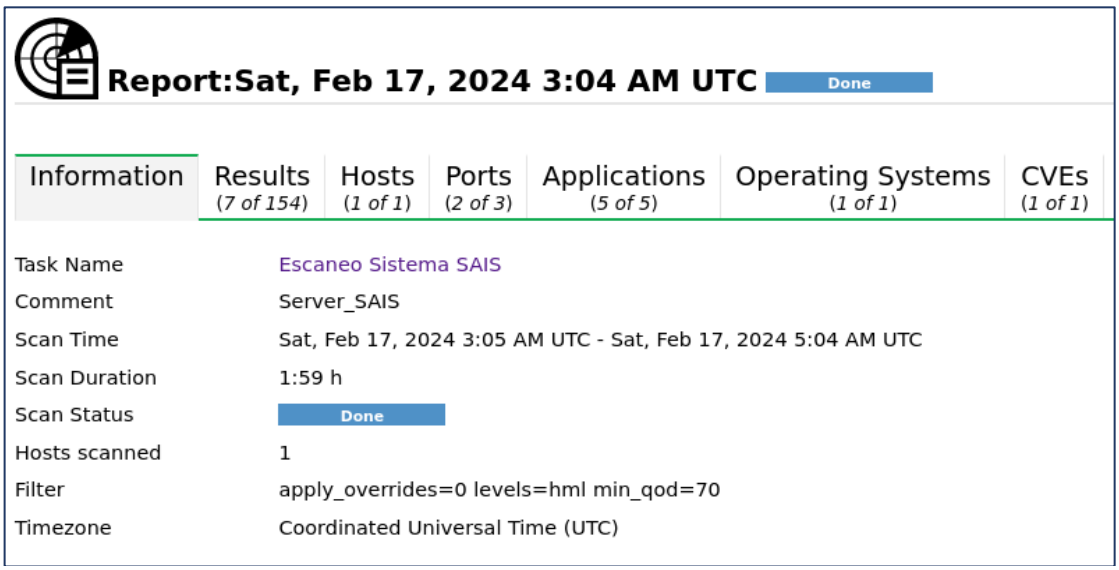
Nota: Características de equipo Sistema SAIS

3.2 Escaneo de Vulnerabilidades

Se visualiza a continuación el reporte obtenido del escaneo realizado en el equipo servidor_sais el mismo que aloja el sistema de atención médica, mediante la Herramienta OpenVAS (*instalación y configuración adecuada en anexo*)

Figura 4

Reporte General de primer escaneo



Nota. Tomada de la herramienta OpenVAS.

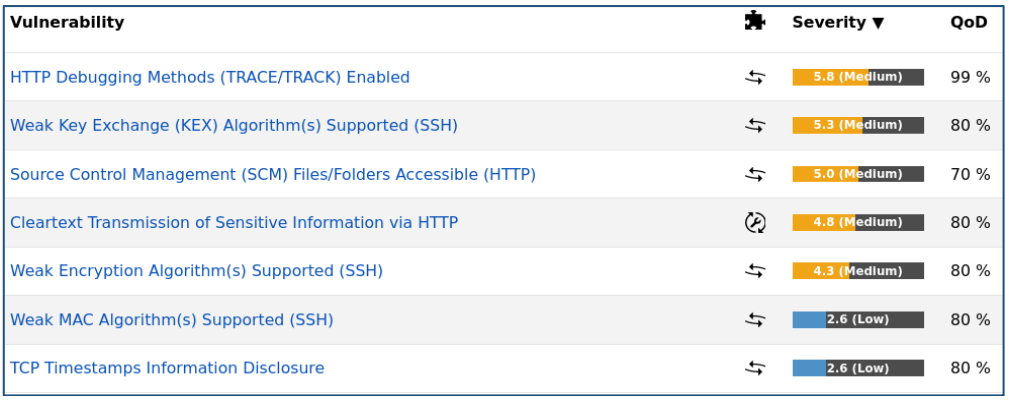
En la gráfica podemos observar el primer escaneo realizado, el mismo que indica los resultados del proceso de evaluación, numero de host o equipo, puertos que considera

en riesgo, el tipo de sistema operativo encontrado y listado de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación.

RESULTADO DEL ESCANEO

Figura 5

Reporte de vulnerabilidades del primer escaneo



Vulnerability	Severity ▼	QoD
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %
Source Control Management (SCM) Files/Folders Accessible (HTTP)	5.0 (Medium)	70 %
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	80 %
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	80 %
TCP Timestamps Information Disclosure	2.6 (Low)	80 %

Nota. Tomada de la herramienta OpenVAS

VULNERABILIDAD 1:

HTTP Debugging Methods (TRACE/TRACK) enabled.

Resumen

El servidor web remoto admite METODOS TRACE y/o TRACK. Son métodos HTTP que se utilizan para depurar conexiones de servidores web.

Resultado de la detección

El servidor web tiene habilitados los siguientes métodos HTTP: TRACE

Base de conocimiento

Se ha demostrado que los servidores web que soportan estos métodos están sujetos a ataques de secuencias de comandos entre sitios, denominados XST por Cross-Site-Tracing, cuando se utilizan en conjunto con varias debilidades en los navegadores.

Método de detección

Comprueba si los métodos HTTP como TRACE y TRACK están habilitado y se puede utilizar.

Detalles: Métodos de depuración HTTP (TRACE/TRACK) OID habilitado: 1.3.6.1.4.1.25623.1.0.11213

Versión utilizada: 2023-08-01T13:29:10Z

Software/SO afectado

Servidores web con métodos TRACE y/o TRACK habilitados.

Impacto

Un atacante puede utilizar este fallo para engañar a su web legítima de usuarios que le den sus credenciales.

Solución

Tipo de solución: Mitigación

Deshabilite los métodos TRACE y TRACK en la configuración del servidor web.

Referencias:

CVE	CVE-2003-1567
	CVE-2004-2320
	CVE-2004-2763
	CVE-2005-3398
	CVE-2006-4683
	CVE-2007-3008
	CVE-2008-7253
	CVE-2009-2823
	CVE-2010-0386
	CVE-2012-2223
	CVE-2014-7883
CERT	DFN-CERT-2021-1825
	DFN-CERT-2014-1018
	DFN-CERT-2010-0020

CB-K14/0981

Other http://www.kb.cert.org/vuls/id/288308

http://www.securityfocus.com/bid/11604

http://www.securityfocus.com/bid/15222

http://www.securityfocus.com/bid/19915

http://www.securityfocus.com/bid/24456

http://www.securityfocus.com/bid/33374

http://www.securityfocus.com/bid/36956

VULNERABILIDAD 2:

Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)

El servidor SSH remoto está configurado para permitir/soportar claves débiles algoritmo(s) de intercambio (KEX).

Resultado de la detección

El servidor SSH remoto admite los siguientes algoritmos KEX débiles:

Figura 6

Algoritmos KEX weak

```
KEX algorithm                     | Reason
----------------------------------------------------------------------------------------
diffie-hellman-group-exchange-sha1 | Using SHA-1
diffie-hellman-group1-sha1         | Using Oakley Group 2 (a 1024-bit MODP group) and SHA-1
```

Nota. Tomada de herramienta OpenVAS

Base de conocimiento

- Grupo MODP de 1024 bits/algoritmos KEX principales:

Millones de servidores HTTPS, SSH y VPN utilizan los mismos números primos para la clave Diffie-Hellman intercambio. Los profesionales creían que esto era seguro siempre que se generaran nuevos mensajes de intercambio de claves para cada conexión. Sin embargo, el primer paso en el tamiz del campo numérico, el más eficiente. El algoritmo para romper una conexión Diffie-Hellman depende sólo de este factor primo. Un nation-state puede romper un número primo de 1024 bits.

Método de detección

Comprueba los algoritmos KEX admitidos del servidor SSH remoto.

Los algoritmos KEX débiles actualmente se definen de la siguiente manera:

- Algoritmos KEX Diffie-Hellmann (DH) de curva no elíptica con grupo MODP/prime de 1024 bits
- Los grupos de intercambio de claves generados efímeramente utilizan SHA-1
- Usando clave de módulo RSA de 1024 bits

Detalles:

Algoritmo(s) de intercambio de claves débiles (KEX) admitidos (SSH) OID: 1.3.6.1.4.1.25623.1.0.150713

Versión utilizada:2023-10-12T05:05:32Z

Impacto

Un atacante puede romper rápidamente conexiones individuales.

Solución

Tipo de solución: Mitigación

Deshabilite los algoritmos KEX débiles informados

Referencias de la vulnerabilidad

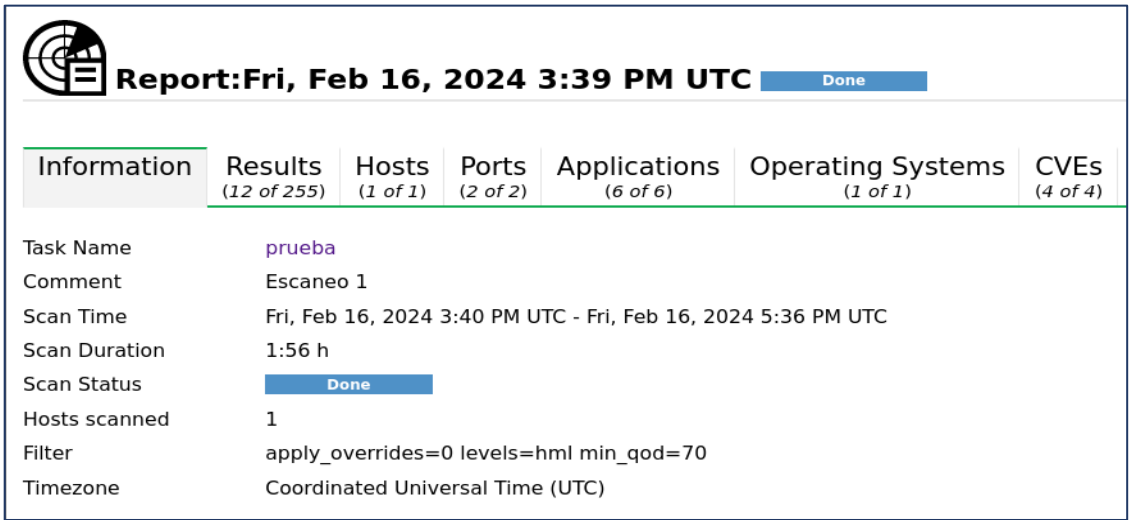
https://weakdh.org/sysadmin.html
https://www.rfc-editor.org/rfc/rfc9142
https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem
https://www.rfc-editor.org/rfc/rfc6194
https://www.rfc-editor.org/rfc/rfc4253#section-6.5

Se visualiza a continuación el reporte obtenido del escaneo realizado, en el equipo Proxy Server, el mismo que aloja el módulo de un sistema de inventario / bodega y Aplicativo

Referencias, Firewall; mediante la Herramienta OpenVAS (*instalación y configuración adecuada en anexo*)

Figura 7

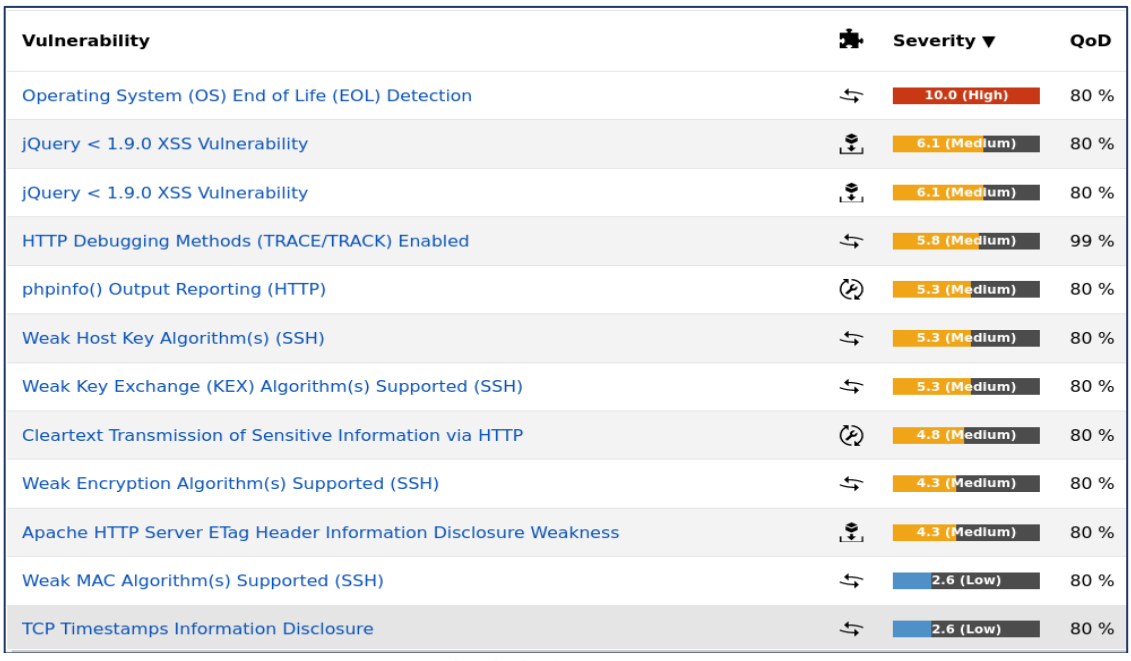
Reporte General de segundo escaneo



Nota. Tomada de la herramienta OpenVAS

Figura 8

Detalle de vulnerabilidades segundo escaneo



Nota. Tomada de la herramienta OpenVAS

3.2.1 Detalle de vulnerabilidades en la infraestructura de red

Tabla 5

Matriz de Vulnerabilidades encontradas

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
HTTP Debugging Methods (TRACE/TRACK) enabled	5.8 Medio	99%	El servidor web tiene habilitados los siguientes métodos HTTP: TRACE	Se ha demostrado que los servidores web que soportan estos métodos están sujetos a ataques de secuencias de comandos entre sitios, denominados XST por Cross-Site-Tracing, cuando se utilizan en conjunto con varias debilidades en los navegadores	Comprueba si los métodos HTTP como TRACE y TRACK están habilitado y se puede utilizar	2023-08-01T13:29:10Z	Un atacante puede utilizar este fallo para engañar a su web legítima de usuarios que le den sus credenciales	CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253 CVE-2009-2823 CVE-2010-0386 CVE-2012-2223 CVE-2014-7883
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 Medio	80%	El servidor SSH remoto admite los siguientes algoritmos KEX débiles	Millones de servidores HTTPS, SSH y VPN utilizan los mismos números primos para la clave Diffie-Hellman intercambio. Los	Comprueba los algoritmos KEX admitidos del servidor SSH remoto.	2023-10-12T05:05:32Z	Un atacante puede romper rápidamente conexiones individuales.	https://weakdh.org/sysadmin.html https://www.rfc-editor.org/rfc/rfc9142

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
				profesionales creían que esto era seguro siempre que se generaran nuevos mensajes de intercambio de claves para cada conexión. Sin embargo, el primer paso en el tamiz del campo numérico, el más eficiente. El algoritmo para romper una conexión Diffie-Hellman depende sólo de este factor primo. Un nation-state puede romper un número primo de 1024 bits.	Los algoritmos KEX débiles actualmente se definen de la siguiente manera: •Algoritmos KEX Diffie-Hellmann (DH) de curva no elíptica con grupo MODP/prime de 1024 bits •Los grupos de intercambio de claves generados efímeramente utilizan SHA-1 •Usando clave de módulo RSA de 1024 bits			https://www.rfc-editor.org/rfc/rfc9142#name-summary-guidance-for-implem https://www.rfc-editor.org/rfc/rfc6194 https://www.rfc-editor.org/rfc/rfc4253#section-6.5
EQUIPO PROXY | SERVER | MODULO BODEGA								
Operating System (OS) End of Life (EOL) Detection	10.0 ALTO	80%	El sistema operativo "CentOS" del host remoto ha llegado al final de su vida útil.	Información de EOL: http://wiki.centos.org/Download El sistema operativo (SO) en el host remoto ha llegado al final de soporte (EOL) y no debe usarse más.	Comprueba si hay una versión EOL de un sistema operativo en el objetivo anfitrión. Detalles: Sistema operativo (SO) Detección de fin de vida	2022-04-05T13:00:52Z	Una versión EOL de un sistema operativo no recibe ninguna actualización de seguridad del vendedor. Un	

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
			CPE: cpe:/o:centos:centos:6 Versión instalada construcción o SP: 6 Fecha EOL: 2020-11-30		útil (EOL) OID: 1.3.6.1.4.1.25623.1.0.103674		atacante podría aprovechar las vulnerabilidades de seguridad no solucionadas para comprometerlas la seguridad de este anfitrión	
jQuery < 1.9.0 XSS Vulnerability	6.1 Medio	80%	jQuery es propenso a secuencias de comandos entre sitios (XSS) vulnerabilidad	La función jQuery(strInput) no diferencia selectores desde HTML de forma fiable. En versiones vulnerables, jQuery determina si la entrada era HTML buscando el carácter '<' en cualquier parte de la cadena, lo que brinda a los atacantes más flexibilidad al intentar construir una carga útil maliciosa. En versiones fijas, jQuery solo considera	Comprueba si hay una versión vulnerable en el host de destino. Detalles: jQuery < 1.9.0 Vulnerabilidad XSS OID: 1.3.6.1.4.1.25623.1.0.141636	2023-07-14T05:06:08Z		CVE-2012-6708 DFN-CERT-2023-1197 DFN-CERT-2020-0590 WID-SEC-2022-0673 CB-K22/0045 CB-K18/1131

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
				la entrada HTML si comienza explícitamente con el carácter '<', limitando la explotabilidad sólo a atacantes que pueden controlar el comienzo de una cadena, lo cual es mucho menos común.				
HTTP Debugging Methods (TRACE/TRACK) enabled	5.8 Medio	80%	El web server tiene habilitados los siguientes métodos HTTP: TRACE	Se ha demostrado que los servidores web que soportan estos métodos están sujetos a ataques de secuencias de comandos entre sitios, denominados XST por Cross-Site-Tracing, cuando se utilizan en conjunto con varias debilidades en los navegadores	Comprueba si los métodos HTTP como TRACE y TRACK están habilitado y se puede utilizar	2023-08-01T13:29:10Z	Un atacante puede utilizar este fallo para engañar a su web legítima de usuarios que le den sus credenciales.	CVE-2003-1567 CVE-2004-2320 CVE-2004-2763 CVE-2005-3398 CVE-2006-4683 CVE-2007-3008 CVE-2008-7253
phpinfo () Output Reporting (HTTP)	5.3 Medio	80%	Archivos llaman a la función phpinfo () que revela	Muchos tutoriales de instalación de PHP instruyen al usuario a crear un archivo llamado phpinfo.php o	Este script informa sobre archivos identificados por los siguientes VT: 'phpinfo () Detección de salida (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).	2023-12-14T08:20:35Z	Parte de la información que se puede	CVE-2008-0149 CVE-2023-49282 CVE-2023-49283

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
			información potencialmente confidencial	similar que contiene la declaración phpinfo (). Un archivo de este tipo a menudo se deja nuevamente en el directorio del servidor web	Detalles**:** phpinfo () Informe de salida (HTTP) OID: 1.3.6.1.4.1.25623.1.0.11229		recopilar de este archivo incluye: El nombre de usuario del usuario que ejecuta el proceso PHP, si es un usuario sudo, la dirección IP del host, el servidor web versión, la versión del sistema (Unix, Linux, Windows, ...)	
Algoritmo(s) de clave de host débil (SSH)	5.3 Medio	80%	El servidor SSH remoto está configurado para permitir/soportar hosts débiles		Comprueba los algoritmos de clave de host admitidos del SSH remoto servidor. Los algoritmos de clave de host actualmente débiles se definen de la siguiente manera: -ssh-dss: Algoritmo de firma digital (DSA) / Estándar de firma digital (DSS) •Detalles:	2023-10-12T05:05:32Z		https://www.rfc-editor.org/rfc/rfc8332 https://www.rfc-editor.org/rfc/rfc8709

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
			algoritmo(s) clave.		•Algoritmo(s) de clave de host débil (SSH) OID: 1.3.6.1.4.1.25623.1.0.117687			https://www.rfc-editor.org/rfc/rfc4253#section-6.6
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 Medio	80 %	El servidor SSH remoto está configurado para permitir/soportar claves débiles algoritmo(s) de intercambio (KEX).	Millones de servidores HTTPS, SSH y VPN utilizan los mismos números primos para la clave Diffie-Hellman intercambio. Los profesionales creían que esto era seguro siempre que se generaran nuevos mensajes de intercambio de claves para cada conexión. Sin embargo, el primer paso en el tamiz del campo numérico, el más eficiente el algoritmo para romper una conexión Diffie-Hellman depende sólo de este factor primo	Comprueba los algoritmos KEX admitidos del servidor SSH remoto. Los algoritmos KEX débiles actualmente se definen de la siguiente manera: • Algoritmos KEX Diffie-Hellmann (DH) de curva no elíptica con grupo MODP/prime de 1024 bits. •Los grupos de intercambio de claves generados efímeramente utilizan SHA-1 •Usando clave de módulo RSA de 1024 bits •Detalles: Algoritmo(s) de intercambio de claves débiles (KEX) admitidos (SSH) OID: 1.3.6.1.4.1.25623.1.0.150713	2023-10-12T05:05:32Z	Un atacante puede romper rápidamente conexiones individuales.	
Cleartext Transmission of	4.8 Medio	80%	El host/aplicación	Se identificaron los siguientes campos de entrada	Evalúe la información recopilada anteriormente y verifique si el host/aplicación no es hacer cumplir la	2023-09-07T05:05:21Z	Un atacante podría utilizar	

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
Sensitive Information via HTTP			transmite información sensible (nombre de usuario, contraseñas) en texto claro a través de HTTP	(URL: nombre de entrada): http://42.223.125.200.static.anycast.cnt-grms.ec/phpMyAdmin/:pma_password http://42.223.125.200.static.anycast.cnt-grms.ec/phpMyAdmin/?D=A:pma_password http://42.223.125.200.static.anycast.cnt-grms.ec/phpmyadmin/:pma_password http://42.223.125.200.static.anycast.cnt-grms.ec/phpmyadmin/?D=A:pma_password	transmisión de datos confidenciales a través de una conexión SSL/TLS cifrada. Actualmente el script está comprobando lo siguiente: -Autenticación básica HTTP (autenticación básica) -Formularios HTTP (por ejemplo, inicio de sesión) con campo de entrada de tipo 'contraseña'		esta situación para comprometer o escuchar a escondidas la Comunicación HTTP entre el cliente y el servidor mediante un ataque de intermediario para obtener acceso a datos confidenciales como nombres de usuario o contraseñas	
Weak Encryption Algorithm(s) Supported (SSH)	4.3 Medio	80 %	El servidor SSH remoto admite los siguientes algoritmos débiles de	El cifrado 'arcfour' es el cifrado de flujo Arcfour con 128 bits llaves. El cifrado Arcfour es compatible con el cifrado RC4, estos tienen	Comprueba los algoritmos de cifrado admitidos (cliente a servidor y de servidor a cliente) del servidor SSH remoto.	2023-10-12T05:05:32Z		

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
			cifrado de cliente a servidor: 3des-cbc aes128-cbc aes192-cbc aes256-cbc arcfour128 arcfour256 blowfish-cbc	problemas con claves débiles y no debería usarse más. -El algoritmo 'ninguno' especifica que no se debe realizar ningún cifrado. Se debe considerar que en este método no existe protección de confidencialidad por lo que no es recomendable más su uso. -Existe una vulnerabilidad en los mensajes SSH que emplean el modo CBC que puede permitir a un atacante recuperar texto sin formato de un bloque de texto cifrado.	Los algoritmos de cifrado actualmente débiles se definen de la siguiente manera: -Algoritmos basados en cifrado Arcfour (RC4) -algoritmo 'ninguno' -Algoritmos basados en cifrado en modo CBC Detalles: Algoritmos de cifrado débiles admitidos (SSH) OID: 1.3.6.1.4.1.25623.1.0.105611			
Apache HTTP Server ETag Header Information	4.3 Medio	80%	Se ha descubierto una debilidad en el servidor HTTP Apache si está	Producto cpe:/a: apache: http_servidor:2.2.15 Método Consolidación de detección del servidor HTTP Apache (OID:	Debido a la forma en que genera el servidor Apache HTTP Encabezados de respuesta ETag, es posible que un atacante obtenga información	2022-12-05T10:11:03Z	La explotación de este problema puede proporcionar a un atacante	CVE-2003-1418 CERT DFN-CERT-2017-1821 DFN-CERT-2017-0925

VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
Disclosure Weakness			configurado para utilizar la directiva FileETag	1.3.6.1.4.1.25623.1.0.117232)	confidencial con respecto a los archivos del servidor. Específicamente, los campos de encabezado de ETag devueltos a un cliente contienen el número de inodo del archivo. Detalles: Debilidad de divulgación de información del encabezado ETag del servidor HTTP Apache OID: 1.3.6.1.4.1.25623.1.0.103122		información que puede usarse para lanzar más ataques contra una red objetivo	DFN-CERT-2015-0495 CB-K17/1750 CB-K17/0896 CB-K15/0469
Weak MAC Algorithm(s) Supported (SSH)	2.6 Bajo	80 %	El servidor SSH remoto está configurado para permitir/soportar MAC débil algoritmo(s).		Comprueba los algoritmos MAC admitidos (cliente a servidor y servidor a cliente) del servidor SSH remoto. Los algoritmos MAC actualmente débiles se definen de la siguiente manera: - Algoritmos basados en MD5 - Algoritmos basados en 96 bits	2023-10-12T05:05:32Z		

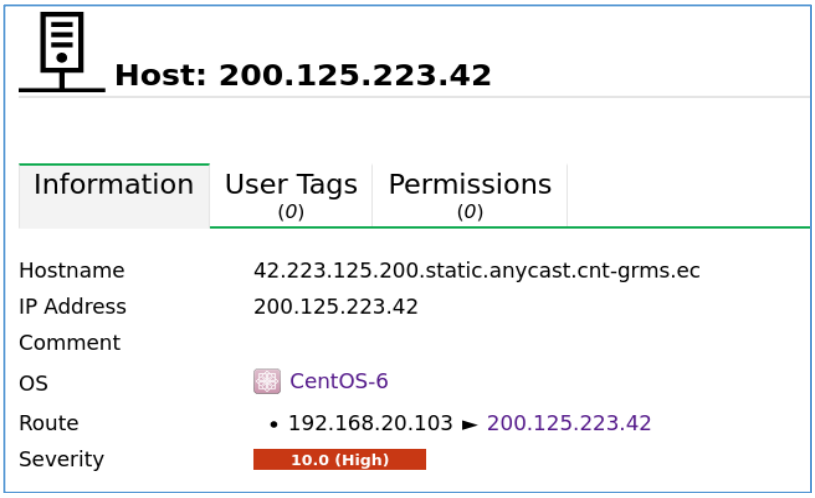
VULNERABILIDAD	NIVEL	QoD	RESULTADO	BASE DE CONOCIMIENTO	METODO DETECCION	VERSION UTILIZADA	IMPACTO	REFERENCIAS
					- Algoritmos basados en 64 bits - algoritmo 'ninguno'			
TCP Timestamps Information Disclosure	2.6 Bajo	80 %	El host remoto implementa marcas de tiempo TCP y por lo tanto permite para calcular el tiempo de actividad	El host remoto implementa marcas de tiempo TCP, según lo definido por RFC1323/RFC7323.	Los paquetes IP especiales se falsifican y envían con un pequeño retraso en entre la IP de destino. Las respuestas se buscan por marcas de tiempo. Si se encuentran, las marcas de tiempo están reportados. Detalles: OID de divulgación de información de marcas de tiempo de TCP: 1.3.6.1.4.1.25623.1.0.80091	2023-12-15T16:10:08Z	Un efecto secundario de esta característica es que el tiempo de actividad del control remoto a veces se puede calcular el host	https://datatracker.ietf.org/doc/html/rfc1323https://datatracker.ietf.org/doc/html/rfc7323https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152https://www.fortiguard.com/psirt/FG-IR-16-090

Nota: Resultados de Vulnerabilidades encontradas

3.2.2 Análisis de puertos comprometidos

Figura 9

Resultados de escaneo de puertos

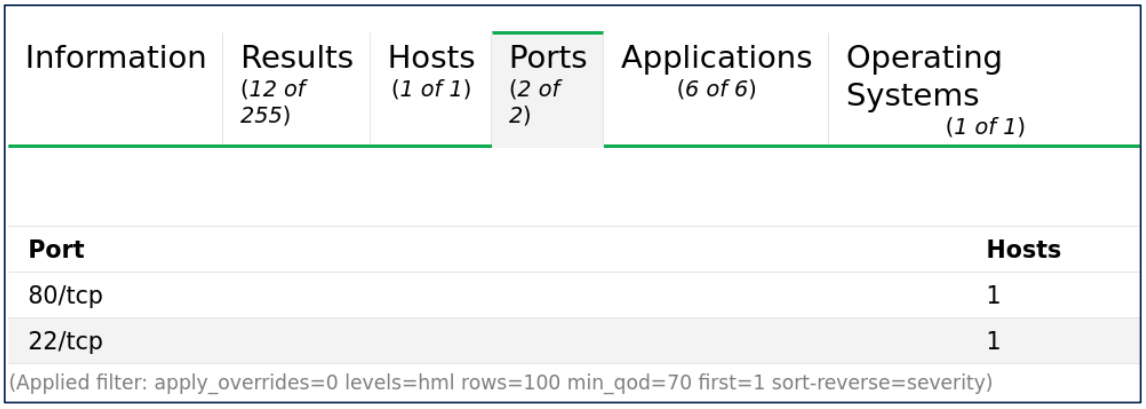


Nota. Tomada de la herramienta OpenVAS

Dentro del análisis desarrollado se puede observar los puertos vulnerables por encontrarse expuestos como son: 80, 22

Figura 10

Reporte de puertos vulnerables



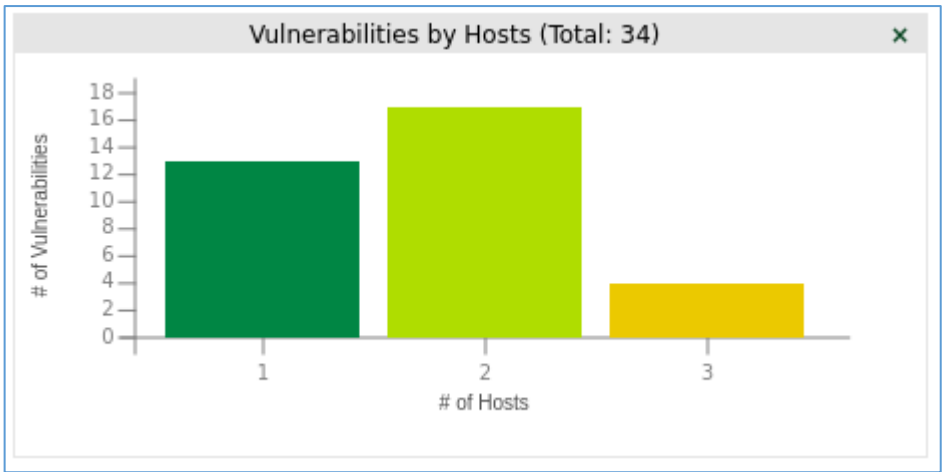
Nota. Tomada de la herramienta OpenVAS

ANÁLISIS DE VULNERABILIDADES

En la siguiente ilustración observamos el total de equipos a los cuales se sometieron a los escaneos de vulnerabilidades realizados dentro de la herramienta OpenVAS, total de 3 equipos de la infraestructura.

Figura 11

Resultado de escaneos



Nota. Tomada de la herramienta OpenVAS

El mismo que de acuerdo con la herramienta, clasifica el nivel de Riesgo de la siguiente manera:

Tabla 6

Niveles de riesgo

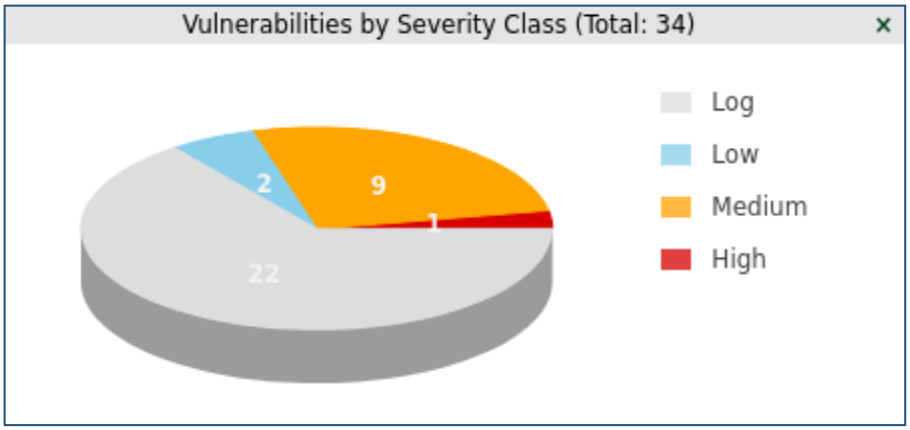
Ítem	Categoría - Nivel
1	Log (información)
2	Bajo
3	Medio
4	Alto

Nota: Niveles de riesgo brindados por herramienta

La ilustración arriba nos muestra el escaneo clasificado como Riesgo Alto, el mismo que se ubica en el equipo de red Proxy, con más de 30 vulnerabilidades.

Figura 12

Resultado de Vulnerabilidades por clases de Riesgo

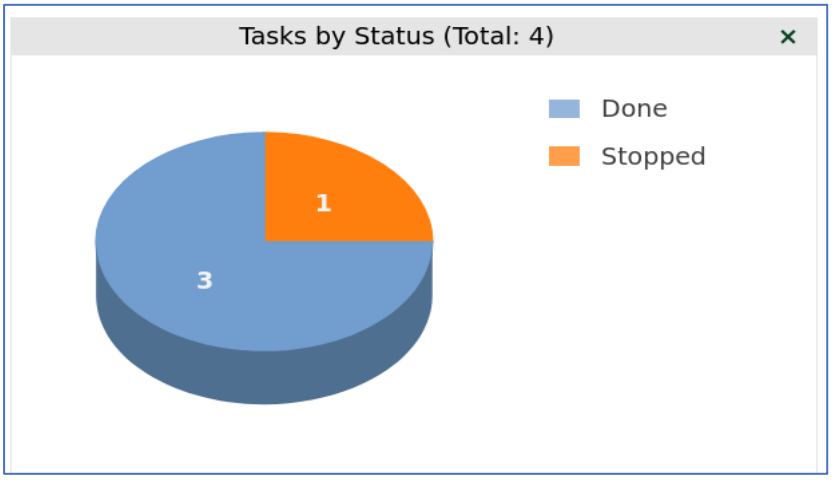


Nota. Tomada de la herramienta OpenVAS

A continuación, la gráfica abajo nos indica que dentro de la herramienta se han desarrollado 4 escaneos, de los cuales 3 se pudieron ejecutar de manera satisfactoria, y uno fue detenido debido a que el equipo de comunicación objetivo no era propiedad de la entidad, sin embargo, pertenecía a la infraestructura como tal.

Figura 13

Total de Escaneos

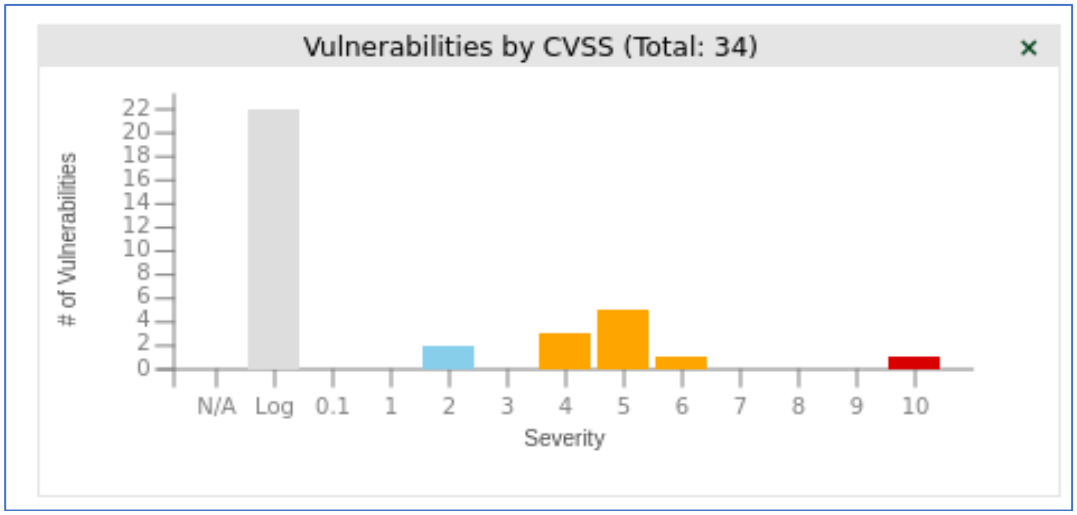


Nota. Tomada de la herramienta OpenVAS

Se obtuvo un total de 34 vulnerabilidades encontradas en los escaneos realizados.

Figura 14

Resultado de Vulnerabilidades por CVSS



Nota. Tomada de la herramienta OpenVAS

A continuación, se observan los escaneos realizados con su nivel de riesgo citado por la herramienta OpenVAS.

Figura 15

Total de Escaneos elaborados

Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Escaneo Sistema SAIS	5.8 (Medium)	0	5	2	19	0	
Escaneo Sistema SAIS	N/A	0	0	0	0	0	
ESCANEO_INET	N/A	0	0	0	0	0	
INFRAESTRUCTURA 2	0.0 (Log)	0	0	0	4	0	
INFRAESTRUCTURA	10.0 (High)	1	9	2	22	0	

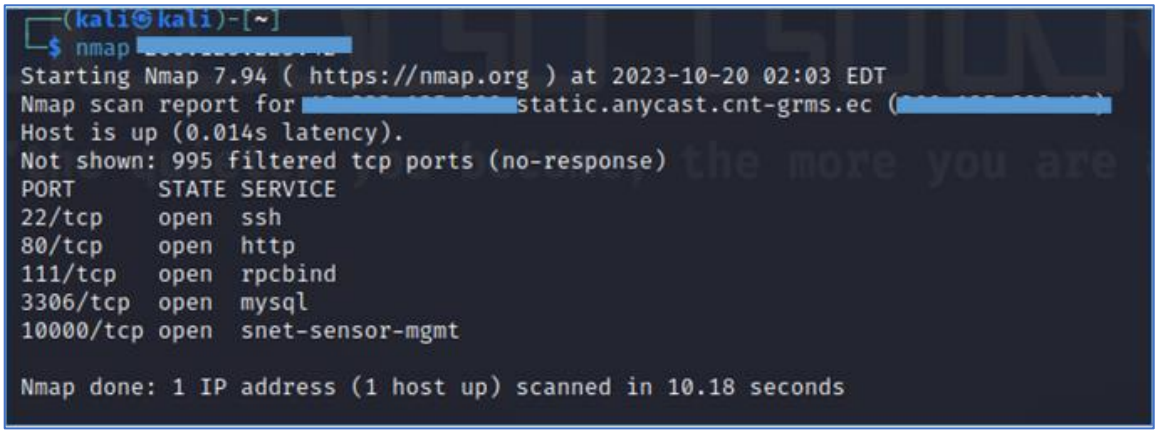
Nota. Tomada de la herramienta OpenVAS

3.2.3 Análisis de Vulnerabilidades Con Nmap.

Se utilizó la herramienta NMAP, paquete que viene ya preinstalado en Kali Linux, por lo que se hizo uso de la aplicación para poder determinar los puertos abiertos para que se tome en consideración y en lo posterior realizar el pan de seguridad en base a los hallazgos:

Figura 16

Resultado de Escaneo con NMAP



Nota. Tomada de la herramienta Kali Linux

La vulnerabilidad encontrada es la versión del sistema operativo, ya que esta se encuentra en una versión anterior sin soporte, adicional de los puertos desprotegidos encontrados, tal como se detalla:

Tabla 7

Puertos abiertos analizados con Nmap

PUERTO	ESTADO	SERVICIO
22	ABIERTO	SSH
80	ABIERTO	HTTP
111	ABIERTO	RPC BIND
3306	ABIERTO	BD MYSQL

PUERTO	ESTADO	SERVICIO
10000	ABIERTO	NET-MGMT

Nota. Descripción de puertos analizados con nmap

3.2.4 Análisis de Vulnerabilidades en el área física donde se encuentra el servidor

En estos momentos el equipo servidor está ubicado en el área de tecnologías, compartida con oficinas administrativas del área y cuyas características se describen a continuación:

Tabla 8

Análisis de Vulnerabilidad a la seguridad Física

ANALISIS DE VULNERABILIDAD EN ÁREA FISICA DEL CENTRO DE COMPUTO	
ITEMS DE SEGURIDAD	**CUMPLE SI / NO**
Seguridad en puerta Blindaje	No
Videovigilancia	No
Control biométrico	No
Detección de Humo	No
Generador eléctrico propio	No
UPS	Si
A/A funcionamiento	Si
Piso falso	No
Tomacorrientes polarizadas	Si
Cableado estructurado	No

Nota. Análisis de Vulnerabilidad a la seguridad Física al área TIC

De acuerdo con la tabla arriba, el área de tecnologías en lo que a seguridad física refiere, apenas cumple con 3 ítems del total las especificaciones recomendadas para un funcionamiento adecuado.

3.3 Diseño de Plan de Seguridad basados en norma ISO 27001

En el Caso de Estudio para el análisis de vulnerabilidad y propuesta de Aseguramiento de la Seguridad de la información, Mejía define que, dentro del enfoque administrativo de este tipo de proyecto prácticos de seguridad, se define la necesidad de establecer las bases para la implementación de un SGSI, basados en la norma ISO/IEC 27001.(Mejía, 2020).

Por lo que, dentro de la propuesta de solución para la mejora de la seguridad, está el definir el diseño de un plan de seguridad de la infraestructura de red destacando las mejores prácticas basados en la norma citada anteriormente.

Posterior al desarrollo del plan de seguridad citado anteriormente, podemos determinar que se puede implementar medidas preventivas y de protección para mitigar las vulnerabilidades y fortalecer esta seguridad a partir de los hallazgos encontrados, por lo que se verifica de manera positiva la hipótesis inicial, que: *La implementación de medidas correctivas y preventivas según la norma ISO 27001 permitirá identificar y mitigar las vulnerabilidades que puedan afectar a la seguridad de la infraestructura de red del Distrito de Salud.*

Una vez realizado el escaneo y análisis de vulnerabilidades de la infraestructura de red, es meritorio brindar las mejores prácticas de seguridad, las mismas que ayudarán a mitigar las brechas encontradas en el análisis anterior.

La siguiente tabla mostrará las soluciones que deberán ejecutarse para cada vulnerabilidad encontradas en el escaneo.

Tabla 9

Solución a Vulnerabilidades encontradas

Vulnerabilidad	Solución	Tipo de Solución
Operating System (OS) End of Life (EOL) Detection	Actualizar el sistema operativo en el host remoto a una versión que aún sea respaldado y recibiendo actualizaciones de seguridad por parte del proveedor.	Mitigación
jQuery < 1.9.0 XSS Vulnerability	Actualice a la versión 1.9.0 o posterior	Vendorfix
HTTP Debugging Methods (TRACE/TRACK) Enabled	Deshabilite los métodos TRACE y TRACK en la configuración del servidor web.	Mitigación
phpinfo () Output Reporting (HTTP)	Elimine los archivos enumerados o restrinja el acceso a ellos.	Alterna
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	Deshabilite los algoritmos KEX débiles informados	Mitigación
Source Control Management (SCM) Files/Folders Accessible (HTTP)	Restringir el acceso a los archivos/carpetas SCM para sistemas autorizados	Mitigación
Cleartext Transmission of Sensitive Information via HTTP	Hacer cumplir la transmisión de datos confidenciales a través de una conexión SSL/TLS cifrada. Además, asegúrese de que el host/la aplicación redirija a todos los usuarios a la conexión SSL/TLS segura antes de permitiendo ingresar datos	Alterna

Vulnerabilidad	Solución	Tipo de Solución
	confidenciales en las funciones mencionadas	
Apache HTTP Server ETag Header Information Disclosure Weakness	OpenBSD ha lanzado un parche que soluciona este problema. Los números de inodo devueltos por el servidor ahora están codificados usando un hash privado para evitar la divulgación de información sensible.	VendorFix
Weak Encryption Algorithm(s) Supported (SSH)	Deshabilite los algoritmos de cifrado débiles informados	Mitigación
TCP Timestamps Information Disclosure	Para deshabilitar las marcas de tiempo TCP en Linux, se deberá agregar la línea net.ipv4.tcp_timestamps = 0 en el archivo que está en la ruta /etc/sysctl.conf. luego deberá ejecutar 'sysctl -p' para aplicar la configuración en runtime.	Mitigación
Weak MAC Algorithm(s) Supported (SSH)	Para deshabilitar las marcas de tiempo TCP en Linux, se deberá adicionar la línea 'net.ipv4.tcp_timestamps = 0' en el archivo /etc/sysctl.conf., posterior deberá ejecutar 'sysctl -p' para aplicar la configuración en runtime	Mitigación

Nota. Descripción de Solución a Vulnerabilidades encontradas

3.3.1 Esquema de Seguridad

Para un correcto desarrollo del plan de mejoras, se tomó en consideración el nuevo Esquema Gubernamental de Seguridad de la Información EGSI para las instituciones del sector público, el mismo que ha sido estructurado por tres guías y cada una hace referencia a los estándares más importantes para la gestión de la Seguridad como la ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, publicado el 01 de marzo del presente año en el *Tercer Suplemento N.º 509 - Registro Oficial*, de los cuales se escogieron los ítems considerados idóneos para la elaboración de un plan de mejoras para asegurar la información en la entidad de Salud.

La implementación del EGSI está determinado por las necesidades y objetivos de la entidad estatal, la criticidad, los requerimientos de seguridad, los métodos utilizados y la estructura de la entidad pública. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

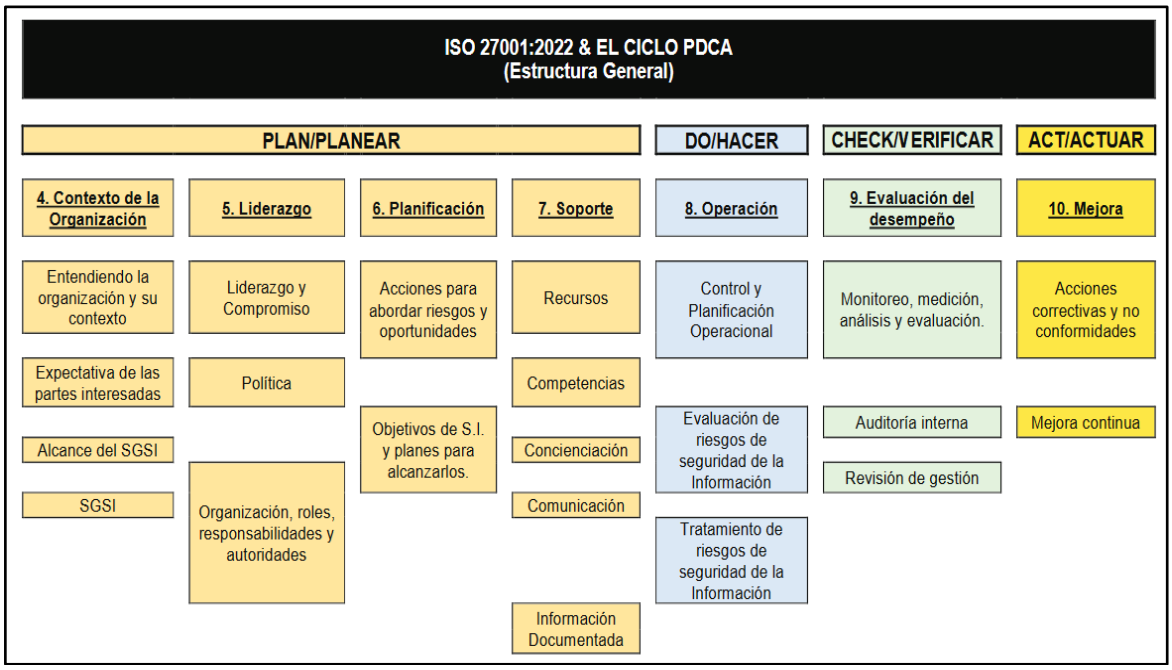
El EGSI salvaguarda la confidencialidad, integridad y disponibilidad de la información a través de una adecuada evaluación de riesgos de seguridad, que aprueba la elección y ejecución de controles para transformar los riesgos identificados y suministrar de servicios seguros al eje principal que es la ciudadanía. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

3.3.2 Plan de mejora

Mediante este plan se recomienda proveer las directrices a la entidad de Salud, para que inicie la implementación del EGSI a través de un proceso constante de mejora.

Figura 17

Estructura PDCA-ISO 27001



Nota. Fuente: EGSI 2024 MINTEL

PLAN PARA LA GESTION DE RIESGOS DE SEGURIDAD:

Se deben considerar los siguientes elementos para iniciar las diferentes acciones de la gestión de riesgo como tal.

Tabla 10

Proceso Gestión de Riesgo de Seguridad de la Información

ACCIONES	PUNTOS POR TRATAR
Establecimiento del contexto	1. Consideraciones Generales organizativas - Levantamiento de información inicial, definición del alcance 2. Establecer criterios básicos de las partes interesadas.

ACCIONES	PUNTOS POR TRATAR
	3. ejecución de la evaluación 4. Establecer criterios de riesgos de seguridad.
Evaluación del Riesgo	**Identificación del riesgo** 5. Identificar los activos de información 6. Identificar las vulnerabilidades **Análisis de riesgos** 7. Determinar consecuencias 8. Evaluación de las consecuencias y la probabilidad de incidentes 9. identificar el nivel de riesgo
Tratamiento del Riesgo	10. Determinar controles
Comunicación y consulta del Riesgo	11. Consultar el riesgo con las partes interesadas en las diferentes etapas del proceso de gestión.
Seguimiento y Revisión del Riesgo	12. Monitorear los riesgos con su respectiva revisión.
Información Documentada	13. Mantener Información documentada sobre el proceso de evaluación de riesgos.

Nota. Proceso Gestión de Riesgo de SI, (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

MONITOREO Y REVISIÓN DE LOS FACTORES DE RIESGO

Es necesario el monitoreo continuo para detectar los diferentes cambios y esta actividad se puede respaldar en servicios externos que permitan obtener información sobre nuevas vulnerabilidades. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Las entidades gubernamentales deben certificar que se cumpla el monitoreo en los ítems siguientes:

Los nuevos activos están dentro del alcance de la gestión de riesgos, cambios necesarios en los valores de los activos. No se han evaluado las nuevas amenazas que pueden estar ocurriendo tanto dentro como fuera de la entidad pública. La probabilidad de que vulnerabilidades nuevas o aumentadas permitan que las amenazas exploten estas nuevas o modificadas, la identificación de vulnerabilidades le permite determinar quién es vulnerable a amenazas nuevas o emergentes, el mayor impacto o consecuencias de las amenazas, vulnerabilidades y riesgos evaluados combinados, lo que resulta en un nivel de riesgo inaceptable. En el EGSI elaborado por: (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024) se menciona que los factores que afectan la probabilidad y las consecuencias de las amenazas pueden cambiar, al igual que los factores que inciden la idoneidad o el costo de las diversas opciones de tratamiento. Los cambios importantes que afectan a la institución deberían ser motivo de una revisión más específica. Por lo tanto, las actividades de monitoreo de riesgos deberían repetirse regularmente y las opciones seleccionadas para el tratamiento de riesgos deberían revisarse periódicamente (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

3.3.4 Guía para la implementación de controles de seguridad de la información:

Los elementos visualizados en este documento se escogen conforme a su naturaleza, lo que los hace adaptables a otros tipos de entidades; y estas tienen la flexibilidad de admitir o desconocer uno o más elementos proporcionados según la gestión, adicional, tienen la libertad de construir atributos propios si así lo consideran (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

DESARROLLO:

1. Controles organizacionales

1.1. Políticas de seguridad de la información

Tabla 11

Políticas de seguridad

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTO	CAPACIDADES OPERACIONALES	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Gobernanza	Ecosistema Resiliencia

Nota. Políticas de seguridad EGSI, Fuente: EGSI 2024

CONTROL

Delimitar la políticas de seguridad de la información, además deberán ser admitidas por la autoridad distrital, situadas, notificadas y registradas por el personal del área de tecnologías; así mismo deben ser revisadas en periodos de tiempos planificados y cuando haya cambios característicos (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Recomendaciones:

La máxima autoridad distrital dispondrá la implementación del EGSI en la entidad, tomando en consideración que las empresas públicas donde procesan colaboran y guardan información en medios electrónicos, clasificada como pública, confidencial, y reservada; deberán aplicar el EGSI para delimitar los procesos con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

La autoridad distrital deberá aprobar la Política de seguridad de la información y ante algún cambio, procesado por el funcionario encargado de la seguridad o quien haga sus veces, sea examinada por este personal, delimitando la normativa necesaria para gestionar la seguridad de la información. También la normas de seguridad deberán estar protegidas por políticas específicas del tema según se considere necesario. Las políticas específicas de uno o varios temas deberán estar alineadas a la política de seguridad institucional, la revisión y aprobación corresponderá al personal encargado de la Seguridad de la información. Para garantizar la eficacia del plan de seguridad de la información en la entidad de Salud, estas deberán ser revisadas por lo menos de forma anual y cuando se produzcan existan o ameriten modificaciones a nivel operativo, tecnológico entre otros; estos deberán ser documentados e informados a las partes interesadas (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

1.6. Contacto con grupos de interés especial

Tabla 12

Grupos de interés especial

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo **Correctivo**	Confidencialidad Integridad Disponibilidad	Proteger Responder Recuperar	Gobernanza	Defensa

Nota. Descripción grupos de interés especial, EGSI, Fuente: EGSI 2024

CONTROL

Establecer contacto con grupos de interés, foros de seguridad, así como asociaciones especializadas en seguridad de la información para contribuir a la mejora

del conocimiento. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024), sin descuidar las capacitaciones para actualizaciones.

Recomendaciones:

Para poder establecer el contacto con grupos de intereses se deberá considerar aumentar el conocimiento de las mejores prácticas así como mantenerse al día con información de seguridad, asegurar que los conocimientos sobre seguridad de la información estén actualizados, recibir notificación temprana de alertas, notificaciones y correcciones relacionadas con ataques a vulnerabilidades en la infraestructura de red a instituciones del sector público, acceder al asesoramiento de expertos en temas de seguridad de la información. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Es de vital importancia asegurar y establecer contacto con grupos de interés siendo esta una estrategia para ayudar a la mejora del conocimiento de seguridad de red.

1.9. Inventario de información

Tabla 13

Inventario de información y otros activos

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Identificar	Gestión de Activos	Gobernanza Ecosistema Protección

Nota. Detalle de inventario de información y otros activos asociados, Fuente EGSI 2024

Control

Se deberá elaborar el inventario de información en conjunto con otros activos incluidos los propietarios. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Recomendaciones

Inventario

La entidad de Salud deberá identificar su información en conjunto con otros activos y establecer su importancia en términos de seguridad de la información; Catalogar los activos, en formatos digitales o físicos. Clasificar los activos de Hardware, Catalogar los activos de Software y dentro de esta categoría se encuentran: Sistemas operativos**,** SaaS, mantenimiento de racks, servidores, software de almacenamiento (NAS), telefonía, sistemas de UPS, de aire acondicionado, CCTV. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Sistemas

La Suite ofimática, navegadores, correo electrónico, vídeo conferencia, servidores como proxy, de archivos, mail server, Print server, servidor de aplicaciones, servidor de base de datos. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Soporte de Redes

Clasificar los activos de soporte de redes, aquí es donde se encuentran los patch panel, puntos de red, racks (piso / pared), Switchs de acceso, borde, si existiere gabinete de servidores, puntos de acceso, convertidores, Router, firewall. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

2.3. Concientización en materia de seguridad de la información

Tabla 14

Formación en seguridad de la información

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad del talento humano	Gobernanza y Ecosistema

Nota. Formación en seguridad de la información, EGSI, Fuente: EGSI 2024

Control

Los funcionarios de la entidad estatal y los colaboradores deberán recibir la correspondiente concientización, y formación sobre la seguridad de la información y de manera conjunta las actualizaciones de la política de seguridad de la información y los procedimientos de temas específicos. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Recomendaciones:

Se debe establecer un plan de concientización, y de educación en temas de seguridad de la información que vaya en armonía con las políticas de seguridad de la información de la entidad de salud. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

La formación en seguridad de la información deberá llevarse a cabo de forma periódica. La concientización, la educación y la formación iniciales pueden aplicarse tanto al personal nuevo como también a aquellos que se trasladan a nuevos puestos. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Concientización

Una planificación de concientización idóneo de la seguridad de la información deberá tener como enfoque principal a que los funcionarios sean firmes en sus compromisos con relación a la seguridad y los medios por los que se cumplen esas responsabilidades y debe cumplir con los siguientes aspectos, en conjunto con la responsabilidad de la autoridad y de los colaboradores. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Enseñanza v preparación

La entidad de Salud deberá identificar, elaborar e implementar un plan de capacitación adecuado para los equipos técnicos y demás colaboradores cuyas funciones requieren de un cúmulo de habilidades y experiencias concretas. Si carecen de habilidades, la entidad deberá preocuparse por obtenerlas. Dependiendo del caso deberá considerar asesorarse por consultores; sin descuidar que es de suma importancia que los funcionarios del área de tecnologías deberán mantener actualizados los conocimientos frecuentando a programas de capacitación que permitirán una mejor aplicación del EGSI. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

2.7. Trabajo a distancia

Tabla 15

Trabajo a distancia

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión de activos Información protección Seguridad física Sistema y seguridad de la Red	Protección

Nota: Descripción de Trabajo a distancia, EGSI, Fuente: EGSI 2024

Control

Establecer políticas y medidas de seguridad mientras los funcionarios de la entidad desarrollan sus actividades de manera remota esto con el fin de salvaguardar la información a la que accede, procesa o almacena fuera de las instalaciones del Distrito de Salud. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Recomendaciones:

El *trabajo a distancia* sucede cuando los funcionarios del Distrito desarrollan sus actividades laborales desde algún lugar que se encuentre fuera de las instalaciones de la entidad de Salud, accediendo a las diferentes plataformas y también a la información ya sea esta en forma impresa o electrónica a través de equipos informáticos. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

El Distrito de Salud deberá emitir procedimientos sobre el tema del trabajo a distancia que delimite las condiciones pertinentes y las restricciones que trae consigo, por lo es imprescindible considerar la seguridad física, teniendo en cuenta los componentes de seguridad para el entorno remoto, el acceso virtual que permita el tratamiento y almacenamiento de información en dispositivos personales, cuidar del acceso de personas no autorizadas a recursos en el entorno virtual, la restricción de utilización o acceso a redes consideradas como públicas (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Estos pasos serán fundamentales para lleva a cabo un procedimiento de control a las actividades realizadas de manera remota o virtual.

3. Controles físicos

3.1. Perímetros de seguridad

Tabla 16

Perímetro de Seguridad Físicos

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS DE SEGURIDAD	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad Física	Protección

Nota. *Perímetro de Seguridad Físicos, EGSI, Fuente: EGSI 2024*

Control

La entidad de Salud deberá definir las áreas que contienen información y otros activos para su correcta protección, de esta forma se evitará el acceso no autorizado, así como algún perjuicio y la interrupción a la información del Distrito (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Recomendaciones:

Se mencionan este apartado las directrices que deberán ser tomadas en cuenta para su posterior desarrollo y ejecución para proteger la seguridad en este caso física, los cuales son: definir los perímetros de seguridad, su ubicación; tener perímetros físicamente consistentes en el lugar que contenga instalaciones de tratamiento de información. Los techos, paredes y pisos del área se recomiendan que sean de construcción compacta y los accesos externos deberán estar protegidas de esta forma se evitará el acceso no autorizado mediante dispositivos de control como alarmas, cerraduras; adicional monitorear y probar todas las puertas contra incendios, y realizar la adquisición de alarmas. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

3.4. Monitoreo a la seguridad física

Tabla 17

Monitoreo de Seguridad Físicos

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS DE SEGURIDAD	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo **Detectivo**	Confidencialidad Integridad Disponibilidad	Proteger Detectar	Seguridad Física	Protección Defensa

Nota. Detalla de procedimiento para un Monitoreo de Seguridad Físicos, EGSI, Fuente: EGSI 2024

Control

Las instalaciones del área deberán ser monitoreadas continuamente para detectar accesos físicos no autorizados. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Recomendaciones:

Es fundamental implementar un sistema de vigilancia integral que combine la presencia de guardias, alarmas contra intrusos, cámaras de seguridad y software de gestión de información. Este sistema puede ser administrado por la propia institución o por un proveedor externo especializado. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

El acceso a los edificios que albergan sistemas e infraestructura crítica debe ser objeto de un monitoreo constante. Para ello, se recomienda la instalación y configuración de cámaras de seguridad y un circuito cerrado de televisión, que permitan visualizar y registrar el movimiento de personas dentro y fuera de las instalaciones del Distrito de Salud. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Las áreas de escaso tránsito también deben estar protegidas por alarmas, es crucial mantener la confidencialidad en la implementación de los sistemas de monitoreo, ya que

su divulgación podría facilitar la ocurrencia de robos sin ser detectados. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Con estas recomendaciones es importante resaltar que toda directriz que se logra instaurar es necesario que se mantenga en absoluta reserva para preservar incluso la integridad de las normativas acogidas por la entidad de Salud.

3.11. Servicios de soporte

Tabla 18

Servicios de Soporte

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS DE SEGURIDAD	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo **Detectivo**	Integridad Disponibilidad	Proteger Detectar	Seguridad Física	Protección

Nota. Servicios de Soporte, EGSI, Fuente: EGSI 2024

Control

Las instalaciones de procesamiento de información de la entidad estatal deberán estar protegidas contra cortes o variaciones de energía y otras complicaciones ocasionadas por fallas en los servicios públicos. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Cabe recalcar que, así como se debe proteger la parte física, no se puede dejar de lado al suministro que alimenta a nivel eléctrico a la infraestructura por esa razón se dan las siguientes sugerencias.

Recomendaciones:

Toda entidad privada o pública penden de los servicios necesarios, ejemplo de aquello es la energía eléctrica, las telecomunicaciones, agua potable, alcantarillado, ventilación y aire acondicionado para mantener de manera adecuada sus instalaciones de procesamiento de información. En este sentido el Distrito de Salud deberá asegurarse de

que su infraestructura este dotado de los servicios públicos y entre ellos los sistemas UPS, generador eléctrico, por lo que deberán estar configurados, funcionando, adicional de proveer del mantenimiento preventivo para asegurar su correcto funcionamiento. Asegurarse de que el equipamiento eléctrico esté en una red separada de las instalaciones o estructura del Distrito para mantener la infraestructura funcionando hasta tomar las decisiones pertinentes. Establecer contactos de emergencia los mismos que deberán archivarse y estar a disposición para el personal en caso de un apagón. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Es de vital importancia mantener un esquema para eventuales situaciones de cortes de fluido eléctrico esto con el afán de garantizar el buen desempeño de la infraestructura y salvaguardar la integridad de la información.

3.12. Seguridad del cableado

Tabla 19

Seguridad del Cableado

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS DE SEGURIDAD	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Disponibilidad	Proteger	Seguridad Física	Protección

Nota. Detalle de Pasos para denotar la Seguridad del Cableado, EGSI, Fuente: EGSI 2024

Control

“Los cables que transportan energía, datos o servicios de información de soporte se deben proteger contra intercepciones, interferencias o daños” (MINTEL, 2023)

Cuanto más infraestructura se tenga, mayor responsabilidad trae consigo mantenerla, es por ellos que se debe contar con las correspondientes protecciones y de esta forma garantizar el cumplimiento de la normativa que dicta el Esquema de Seguridad.

Recomendaciones:

Se deben seguir ciertas pautas para garantizar la seguridad del cableado. En primer lugar, se recomienda que las líneas eléctricas y de telecomunicaciones que lleguen a las instalaciones de procesamiento de información estén subterráneas siempre que sea posible, o que cuenten con protección adicional, como protectores de cables en el suelo y postes de servicios públicos. En el caso de cables subterráneos, es importante protegerlos de cortes accidentales mediante el uso de ductos blindados y señalización adecuada. Además, se debe mantener una separación adecuada entre el cableado eléctrico y los cables de comunicaciones para evitar interferencias. Para sistemas críticos, se deben considerar controles adicionales, como la instalación de conductos blindados y el uso de cuartos o cajas cerradas con alarmas en los puntos de inspección y terminación. También se recomienda utilizar blindaje electromagnético para proteger los cables, realizar barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados conectados a los cables, y utilizar cables de fibra óptica cuando sea necesario. Por último, se debe etiquetar cada extremo de los cables con detalles suficientes sobre su origen y destino para facilitar su identificación e inspección física. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024).

Este apartado sin duda es uno de los principales en el que se deberá empezar a desarrollar una vez aprobado el plan por la máxima autoridad ya que permitirá obtener una adecuada clasificación y etiquetado de la infraestructura como tal, todo esto conllevará a la mejora que se necesita y poder cumplir con las normativas dadas por el EGSI.

4. Controles tecnológicos

4.1. Dispositivos de usuario final

Tabla 20

Controles a dispositivo de usuario Final

TIPO DE CONTROL	PROPIEDADES DE LA SI	CONCEPTOS DE SEGURIDAD	CAPACIDADES OPERATIVAS	DOMINIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Gestión de activos Información protección	Protección

Nota. Detalle de Controles a dispositivo de usuario Final, EGSI, Fuente: EGSI 2024

Control

Se deberá implementar y comunicar la política para el manejo de la información almacenada, en los dispositivos de usuario final. (MINTEL, 2023)

Es sumamente importante este punto ya que, sin un adecuado control en los dispositivos de cada funcionario, es posible se pueda filtrar información, cayendo en unas de las más grandes vulnerabilidades que es el trato directo de la información con el usuario final.

Recomendaciones:

La política implementada debe ser comunicada a todo el personal relevante y considerar los siguientes puntos importantes: 1) Determinar el tipo de información y el nivel de clasificación que los dispositivos del usuario final pueden manejar, procesar y soportar. 2) Registrar los dispositivos de usuario final. 3) Registrar los dispositivos móviles que estén debidamente autorizados. 4) Establecer requisitos de protección física. 5) Prohibir la instalación de software, a menos que sea controlado de forma remota por personal de tecnología del Distrito. 6) Establecer requisitos para el software del dispositivo de usuario final y aplicar actualizaciones, se recomienda mantener activa la actualización automática. 7) Establecer reglas para la conexión a servicios de información, redes públicas u otra red fuera de las instalaciones que requiera el uso de un firewall personal. 8) Definir controles y políticas de acceso. 9) Implementar protección contra programa maligno. 10) Realizar y programar copias de seguridad. 11) Regular el

uso de servicios web y aplicaciones web. 12) Regular el uso de dispositivos y memorias extraíbles, así como la opción de desactivar puertos físicos como el USB. (MINTEL, 2023)

Responsabilidad del usuario

Se deberán tomar en cuenta lo siguiente: a) Cerrar sesiones activas en las diferentes plataformas que administra esta unidad de Salud tales como correo, plataformas, módulos, b) Proteger los dispositivos de usuario final y de uso no autorizado con un control físico y un control lógico como un acceso con contraseña, cuando no estén en uso y dejando parametrizado un tiempo recomendado. c) Utilice dispositivos con mayor cuidado en lugares públicos, oficinas abiertas, lugares de reunión y otras áreas no protegidas (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Uso De Dispositivos Personales

Se deberá mantener una separación del uso personal y de trabajo de los dispositivos, incluido el uso de sistemas para respaldar dicha separación y proteger los datos de la entidad en un dispositivo privado. Políticas y procedimientos de temas específicos para prevenir disputas concernientes con los derechos de propiedad intelectual desarrollados en equipos de propiedad privada (MINTEL, 2023).

Conexiones inalámbricas

La entidad de Salud deberá definir los procedimientos para garantizar la configuración de conexiones inalámbricas en otros dispositivos y a partir aquello se proceda a deshabilitar protocolos vulnerables, así como utilizar conexiones inalámbricas o por cable con el ancho de banda apropiado de acuerdo con las políticas instauradas por el personal pertinente. (MINTEL, 2023).

4.20. SEGURIDAD DE REDES

Tabla 21

Seguridad de Redes

TIPO DE CONTROL	PROPIEDADES	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIIOS DE SEGURIDAD
Preventivo **Detectivo**	Confidencialidad Integridad Disponibilidad	Proteger Detectar	Sistema y seguridad de la Red	Protección

Nota. Descripción de Seguridad de Redes, EGSI, Fuente: EGSI 2024

Control

Proteger, administrar y controlar las redes y los dispositivos de red, para proteger la información en los sistemas y aplicaciones (MINTEL, 2023) implementadas en el Distrito de Salud.

Considerar cada una de las recomendaciones siguientes ayudarán a fortalecer a la Seguridad a la infraestructura de Red del Distrito de Salud.

Recomendaciones:

Se deben implementar medidas de seguridad para proteger la información en las redes y su infraestructura, con el objetivo de proteger los servicios conectados contra accesos no autorizados. Para lograrlo, es necesario considerar varios elementos: Determinar el tipo de información que la red puede manejar. Establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red. Mantener la documentación actualizada, incluyendo diagramas de red y copias de seguridad de archivos de configuración de los dispositivos. Establecer controles para proteger la confidencialidad e integridad de los datos que circulan por la infraestructura de red. Implementar controles adicionales o especiales para garantizar la disponibilidad de los servicios de red y los equipos informáticos conectados a la red. Establecer sistemas de

monitoreo para registrar y detectar acciones que puedan afectar la seguridad de la información. (MINTEL, 2023)

Es importante coordinar las actividades de gestión de la infraestructura de red para optimizar el servicio y garantizar la consistencia de los controles en toda la infraestructura de red de la entidad de Salud. También se debe considerar la implementación de sistemas de autenticación en la red, restringir y filtrar la conexión de sistemas a la red utilizando nuevas reglas de firewall, detectar y autenticar la conexión de equipos y dispositivos a la red de la entidad de Salud. (MINTEL, 2023)

Además, se debe considerar el endurecimiento de los dispositivos de red, distribuir los canales de administración de red de otro tráfico de red, aislar temporalmente subredes en caso de un ataque a la red de la entidad de Salud, deshabilitar protocolos de red vulnerables y designar procedimientos y responsabilidades para la gestión de equipos remotos, como el redireccionamiento de puertos y accesos por VPN, incluyendo los diferentes entornos, el área de producción y el área de usuarios finales. (MINTEL, 2023)

Cada una de las recomendaciones dadas permitirán brindar un nivel más seguro a la infraestructura de Red de la Entidad de Salud.

4.21. SEGURIDAD DE LOS SERVICIOS DE RED

Tabla 22

Seguridad de los Servicios de Red

TIPO DE CONTROL	PROPIEDADES	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Sistema y seguridad de la Red	Protección

Nota. Descripción de Seguridad de los Servicios de Red, EGSI, Fuente: EGSI 2024

Control

Los mecanismos de seguridad, los niveles de servicio y los requisitos de los servicios de red se deben identificar, implementar y monitorear, independientemente de si estos servicios se entregan de manera interna o están externalizados. (MINTEL, 2023)

Recomendaciones:

Las medidas de seguridad necesarias para los servicios de seguridad, los niveles y los requisitos de servicio deben ser identificados e implementados por los proveedores de servicios de red, ya sean internos o externos. El Distrito de Salud debe asegurarse de que estos proveedores implementen estas medidas. Las reglas sobre el uso y servicios de red deben configurarse para abarcar aspectos como las redes y servicios a los que se permite acceder, los requisitos de autenticación, los procedimientos de autorización, la administración de redes y los controles tecnológicos y procedimientos para proteger el acceso a las conexiones y servicios de red, incluyendo el uso de tecnologías como VPN o red inalámbrica, y la aplicación de tecnologías como autenticación, cifrado y controles de conexión a la red para garantizar la seguridad de los servicios de red. (MINTEL, 2023)

Cada recomendación brindará los lineamientos necesarios para fortalecer los servicios de seguridad de la infraestructura de red.

4.22. SEPARACIÓN EN LAS REDES

Tabla 23

Separación en las Redes

TIPO DE CONTROL	PROPIEDADES	CONCEPTOS	CAPACIDADES OPERATIVAS	DOMINIIOS DE SEGURIDAD
Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Sistema y seguridad de la Red	Protección

Nota. Descripción de Separación en las Redes, EGSI, Fuente: EGSI 2024

Control

Separar las redes en función de los grupos o áreas definidas, considerando números d usuarios y las diferentes plataformas o sistemas de información. (Telecomunicaciones, Guerrero, Martinez, & Gualotuña, 2024)

Recomendaciones:

Para llevar a cabo la separación de redes, es importante considerar las siguientes recomendaciones: El Distrito de Salud debe gestionar la seguridad de las redes dividiéndolas en dominios de red separados y separándolas de la red pública. Es fundamental documentar esta división identificando las direcciones IP en cada segmento de red. Los dominios pueden elegirse en función de los niveles de confianza, criticidad y sensibilidad, como dominios de acceso público, escritorio, servidor, sistemas de alto y bajo riesgo, junto con unidades organizativas como recursos humanos, finanzas, o una combinación de estos. La separación puede lograrse mediante redes físicamente diferentes o utilizando diferentes redes lógicas. Es crucial controlar el perímetro de la infraestructura de red con dispositivos como puertas de enlace, cortafuegos y enrutadores de filtrado de contenido. Para las redes inalámbricas, se requiere un enfoque específico debido a su cobertura y la posibilidad de quedar al alcance de usuarios maliciosos. (MINTEL, 2023).

Para una correcta separación del entorno inalámbrico, se debe considerar todos los demás accesos como conexiones externas y dividir este acceso de las redes hasta que el acceso pase a través de una puerta de enlace de acuerdo con los controles de red antes de conceder acceso a las diferentes plataformas. (MINTEL, 2023)

RESULTADOS

Mediante el desarrollo de la investigación se obtuvieron los resultados siguientes:

Con relación al enfoque cualitativo se logró recabar la información sobre las diferentes vulnerabilidades que amenazan a la red, así como se logró recopilar la percepción sobre la seguridad informática que posee en estos momentos el Distrito de Salud, esto enmarca la situación actual de la infraestructura de la entidad objeto de estudio.

Las herramientas que fueron utilizadas para el escaneo proporcionaron un análisis preciso de las vulnerabilidades detalladas en este trabajo de investigación, las mismas que deberán ser tratadas para su solución, y poder obtener la mejora en cuanto a mitigación a las debilidades encontradas.

Ante lo citado, adicional se provee un plan de mejora de seguridad para la infraestructura de red del distrito, los mismos que están basados en el esquema de seguridad para empresa pública proporcionada por la entidad pertinente (Telecomunicaciones, 2024), y normados por el estándar ISO 27001.

Por lo anterior expuesto, los tres resultados citados permitirán implementar las medidas preventivas y de protección para mitigar las diferentes vulnerabilidades halladas y de esta forma fortalecer la seguridad de la infraestructura de red del Distrito de Salud.

CONCLUSIONES

Durante el desarrollo del trabajo de investigación se pudo evidenciar el estado actual de la infraestructura de red del Distrito de Salud, por lo que se tuvo una apreciación general pero significativa de sus activos tanto en hardware como en software; así como también se pudo revelar que la entidad de salud no cuenta con procedimientos reales para salvaguardar ni recuperar la información, de tal forma que garanticen la integridad, confidencialidad y disponibilidad de la información.

Es necesario recalcar la información de vulnerabilidades descubiertas en el escaneo realizado con la herramienta seleccionada, esto ayudó a obtener una mejor perspectiva de análisis de las debilidades a nivel de infraestructura, por lo que se convierte en el punto de partida para llevar a cabo la mitigación durante la implementación del plan de mejora.

Mediante este trabajo de investigación se consideró implementar un plan de mejora de seguridad de la información, tomando como referencia la norma internacional ISO 27001:2022 y el Esquema de Seguridad para instituciones públicas, la cual permite llevar a otro nivel la gestión de los riesgos de la seguridad de la información, que pueda ser capaz de mitigar y/o en el mejor de los casos, eliminar riesgos de información.

Mantener una mejora continua del plan basado en la norma ISO 27001 es de vital importancia, para ello se creó procedimientos donde se realizarán monitoreos y revisiones que cubran incidentes por parte del área de tecnologías, y a la vez mediante este análisis se puedan tomar las mejores decisiones, al final se logre aplicar medidas correctivas ante los nuevos desafíos de amenazas que se puedan presentar en la infraestructura, en este mundo cambiante y vertiginoso.

La herramienta OpenVAS ha sido muy útil, al ser OpenSource, es una de las alternativas fuertes en su clase, y es una opción viable, si en el lugar donde se implemente no cuente con el recurso suficiente, por ende, no se permita adquirir una privativa.

RECOMENDACIONES

El área de tecnologías del Distrito de Salud deberá realizar evaluaciones periódicas a su infraestructura, en consecuencia, determinar el nivel de riesgo en sus activos informáticos en el que se encuentre, de tal manera que se pueda conocer un estado actual y evaluar de manera contínua su entorno de seguridad.

Establecer el seguimiento correspondiente para la implementación del plan de seguridad, con el objetivo de mantener una mejora continua del plan, así como realizar revisiones periódicas del plan para asegurar que sigue siendo efectivo, dependiendo de esto se podría implementar nuevas medidas de seguridad en función de las nuevas amenazas y riesgos.

Implementar un plan de comunicación para informar a todo el personal sobre la importancia de las medidas de seguridad, así como realizar charlas y capacitaciones con el objetivo de concientizar el impacto que tiene la seguridad de la información en la institución, difundir material informativo sobre el tema, de tal forma que en la entidad de Salud pueda crear una cultura de seguridad de la información.

Instalar, configurar y mantener actualizada la base de conocimientos de la herramienta de escaneo de tal manera que se consiga un mejor análisis de vulnerabilidades y permitan ejecutar el plan adecuado a la entidad, de esta forma podrá ayudar a una mitigación temporal hasta encontrar soluciones a largo plazo dependiendo del tipo de vulnerabilidad en la que se encuentre.

Un plan de seguridad de red basado en ISO/IEC 27001, junto con las mejores prácticas, puede ayudar a proteger la infraestructura de red de la entidad de salud de manera efectiva. Por tal motivo es importante recordar que la seguridad de la información es un proceso continuo que requiere siempre revisión y mejora constante.

REFERENCIAS

Ávila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, *24*(49). https://doi.org/10.15517/isucr.v24i49.50765

Carrión-Barco, G., Sánchez-Chero, M.-J., Del Castillo Castro, C. I., Campos Flores, F. W., & Timaná Álvarez, M. (2021). Modelo de seguridad informática para un medio de conexión pública. *Revista de La Universidad Del Zulia*, *12*(32). https://doi.org/10.46925//rdluz.32.21

Ch, R. (2020). Vulnerability Assessment Using Nessus Tool. In *A Closer Look at Cybersecurity and Cryptanalysis* (pp. 49–62). Nova Science Publishers, Inc.

CISCO. (2023). *¿Que es un firewall?* Cisco Systems, Inc.

Cisco. (2023). *Seguridad de red*. Seguridad de Red.

Cuadros Navarro, C. G., Veliz Briones, V. F., Veloz Zambrano, J. L., & Cruz Felipe, M. del R. (2022). Seguridad Ofensiva Mediante Hacking Ético para Fortalecer Infraestructuras en Redes de Telecomunicaciones. *Serie Científica de La Universidad de Las Ciencias Informáticas, ISSN-e 2306-2495, Vol. 15, Nº. 1, 2022 (Ejemplar Dedicado a: Enero), Págs. 40-53*, *15*(1).

Dr. Vladimir, V. F. (2021). IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA CON LA NORMA ISO/IEC 27001 EN LA EMPRESA RANSA COMERCIAL S.A - PIURA; 2021. In *Gastronomía ecuatoriana y turismo local.* (Vol. 1, Issue 69).

Fernando Ávila Pesantez, D., Chalan Analuisa, R., Figueras, G., & Ávila, M. (2022). Cybersecurity Policies for Network Switching Devices in Hospital Data Centers: A Case Study. *ESPOCH Congresses: The Ecuadorian Journal of S.T.E.A.M.* https://doi.org/10.18502/espoch.v2i2.11413

Flores Robaina, R., Ramírez Pérez, J., & Muñoz Morejón, M. (2021). Rediseño de la infraestructura de red local del Centro de Investigaciones Médico-Quirúrgicas (CIMEQ). Cuba Redesign Local Network Infrastructure of CIMEQ. Cuba. *Revista Cubana de Informática Médica*, *13*(1).

Gilces Zambrano, A. F., Demera Centeno, V., & Vaca Cárdenas, L. (2021). Mecanismos de ciberseguridad basados en honeypots. *Informática y Sistemas: Revista de Tecnologías de La Informática y Las Comunicaciones*, *5*(2). https://doi.org/10.33936/isrtic.v5i2.3708

Guevara-Vega, E. M. D., Delgado-Deza, J. R., & Mendoza-de-los-Santos, A. C. (2023). Vulnerabilidades y amenazas en los activos de información. *Revista Científica de Sistemas e Informática*, *3*(1). https://doi.org/10.51252/rcsi.v3i1.461

Kaspersky Lab. (2021). *¿Qué son los ataques DDoS?* Kaspersky.

Mayorga, A. (2018). Lineamientos, Tendencias y Estrategias sobre Ciberseguridad y Ciberdefensa en Colombia. *Universidad Piloto de Colombia*.

Mejía, A. (2020). Caso De Estudio Para El Análisis De Vulnerabilidad Y Propuesta De Aseguramiento De La Seguridad De La Información En La Infraestructura Tecnológica De La Empresa Nostradamus S.a.S [UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA]. In *Journal of Chemical Information and Modeling* (Vol. 21, Issue 1). https://repository.unad.edu.co/bitstream/handle/10596/34626/amejiaes.pdf?sequence=1&isAllowed=y

Muñoz-Zambrano, C., & Zambrano-Rendón, A. D. (2023). Security Operations Center, como modelo de gestión de ciberseguridad para el Hospital Especialidades de Portoviejo, Manabí-Ecuador. *MQRInvestigar*, *7*(3). https://doi.org/10.56048/mqr20225.7.3.2023.3220-3236

Ortiz-Lazo, J. E., & Vizñay-Duran, J. K. (2019). Análisis de riesgo y vulnerabilidades de la red de datos, en un ISP, utilizando el estándar ISO/IEC 2007:2008. Caso de estudio: Empresa Sistelcel. *Polo Del Conocimiento*, *4*(7). https://doi.org/10.23857/pc.v4i7.1029

Otilia Mosquera-Chere, S. I. (2021). Experiencias de seguridad cibernética en países europeos y latinoamericanos. Apuntes hacia la defensa nacional. *Polo Del Conocimiento*, *6*(3).

Paredes, M. (2022). *¿Qué es el cifrado de datos?* LinkedIn.

Prakash, A., & Kumar, U. (2018). Authentication Protocols and Techniques A Survey. *International Journal of Computer Sciences and Engineering*, *6*(6). https://doi.org/10.26438/ijcse/v6i6.10141020

Rahalkar, S. (2019). OpenVAS. In *Quick Start Guide to Penetration Testing* (pp. 47–71). Apress. https://doi.org/10.1007/978-1-4842-4270-4_2

Ramírez, L. (2020). Diseño y consolidación de un centro de respuesta ante incidentes de seguridad informática en la empresa Cybersecurity de Colombia ITDA. *Journal of Chemical Information and Modeling*, *2*(1).

Rodríguez, O. A. (2018). DISEÑO DE MANUAL BÁSICO DE PRUEBAS DE HACKING ÉTICO: ESCANEO DE RED, DE VULNERABILIDADES Y ATAQUE. *Angewandte Chemie International Edition, 6(11), 951–952.*

Liliana Parra, E. C. (2017). ANÁLISIS DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN. 177.

Narvaez Narvaez, A. E. (2019). *Analisis de Vulnerabilidades para la red LAN de la Empresa HIDROMAG bajo Metodologia OSSTM*. Quito.

Parra Barzola, L. M. (2017). ANÁLISIS DE VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DE UNA EMPRESA, UTILIZANDO HERRAMIENTAS DE TEST DE INTRUSIÓN. 177.

Sulivan, F. &. (2023). Las oportunidades de crecimiento de la ciberseguridad de la salud de EE.UU.

Telecomunicaciones, M. d. (01 de Marzo de 2024). ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION. (R. Oficial, Ed.) 210.

Recursos útiles: Norma ISO/IEC 27001:2022

Sitio web de ISO 27001: https://www.iso.org/isoiec-27001-information-security.html

Guía de implementación de ISO/IEC 27001: https://www.iso.org/publication/PUB100373.html

ANEXOS

Anexo 1: **carta Aval por parte de la entidad objeto del trabajo de investigación**

Gobierno del Ecuador | GUILLERMO LASSO PRESIDENTE

Ministerio de Salud Pública

Coordinación Zonal 5 – Salud
Dirección Distrital 24D01 Santa Elena – Salud

Oficio Nro. MSP-CZS5-SE-24D01-2023-0514-O

Santa Elena, 07 de noviembre de 2023

Asunto: RESPUESTA A SOLICITUD DE AUTORIZACIÓN PARA REALIZAR TRABAJO DE INVESTIGACIÓN EN EL DISTRITO 24D01 SANTA ELENA SALUD - ING. MICHAEL JAIRO BARRERA CRUZ

Sr. Ingeniero
Michaell Jairo Barrera Cruz
En su Despacho

De mis consideraciones:

Reciba cordiales saludos de quienes conformamos el Distrito 24D01 Santa Elena - Salud.

En respuesta al documento S/N ingresado por Ventanilla Única Distrital con el registro No. MSP-CZS5-SE-24D01-VUAU-2023-0609-E, suscrito por Michaell Jairo Barrera Cruz, con C.I. 0921536579, Maestrante de la carrera de Posgrado en la UPSE, en el que solicita autorización para realizar su trabajo de investigación sobre el tema "MONITOREO DE VULNERABILIDADES EN LA INFRAESTRUCTURA DE RED EN EL DISTRITO DE SALUD"

De acuerdo a este contexto, se AUTORIZA al Profesional Michaell Barrera Cruz, realice su trabajo de investigación, en Sede Distrital.

Particular que informo para fines pertinentes.

Atentamente,

Documento firmado electrónicamente

Mgs. Tannia Estefania Cajas Crespo
DIRECTORA DISTRITAL 24D01 SANTA ELENA - SALUD

Referencias:
- MSP-CZS5-SE-24D01-VUAU-2023-0609-E

Copia:
Señorita Magíster
Lorena Alexandra Villon Moreno
Analista Distrital de Soporte Técnico y Redes 3 - 24D01

Anexo 2: **Manual de instalación y configuración correcta de las herramientas.**

DESCARGA E INSTALACION DE HERRAMIENTA DE ANALISIS NESSUS

Para poder realizar el laboratorio, nos dirigimos a la máquina virtual preparada para este fin, el mismo que tiene ya configurada una VM con la distribución Kali Linux 2023.3 amd64. Una vez ya dentro de la VM Kali, nos dirigimos al navegador por defecto Mozilla y digitamos: Download Nessus, luego presionamos tecla enter.

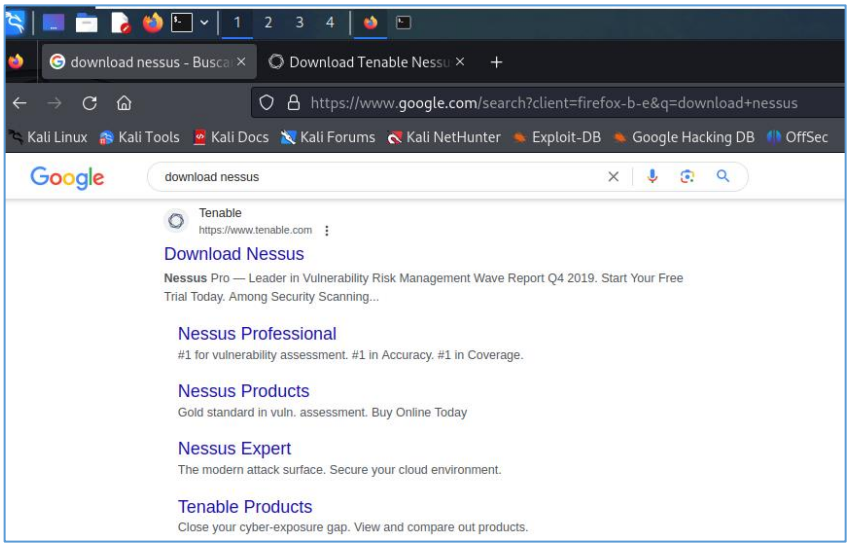


Imagen: búsqueda de herramienta Nessus en buscador

Escogemos la opción por defecto para descargar la versión de Nessus – 10.6.4, damos clic en Download

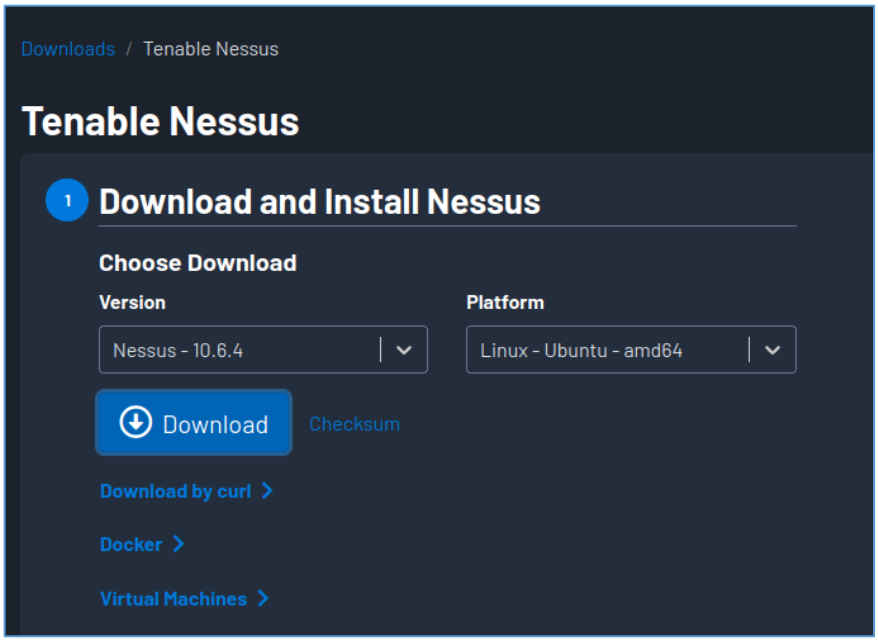


Imagen elección de herramienta Nessus – 10.6.4

Una vez descargado, abrimos el terminal en Kali Linux, y nos dirigimos vía comando a la carpeta Downloads:

$ cd Downloads
$ ls

Con esto podemos visualizar el archivo descargado tal como muestra la gráfica:

Imagen donde muestra la evidencia de descarga de aplicativo Nessus

Ahora procederemos a instalar el paquete descargado mediante el comando:

$ sudo dpkg -i Nessus-10.6.4-ubuntu1404_amd64.deb

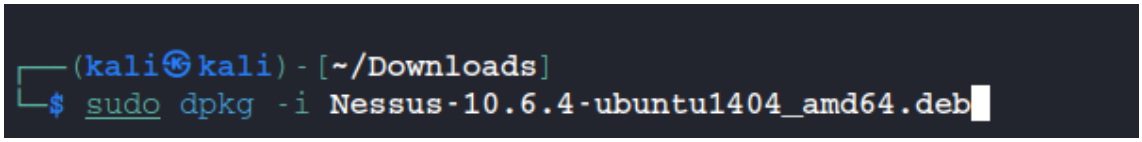


Imagen donde indica comando para instalar Nessus

Luego de instalar la herramienta, procedemos a activar el servicio de Nessus, para lo cual debemos digitar los siguientes comandos:

$ sudo service nessus start
$ sudo service nessus status

A lo que podremos visualizar la siguiente información:

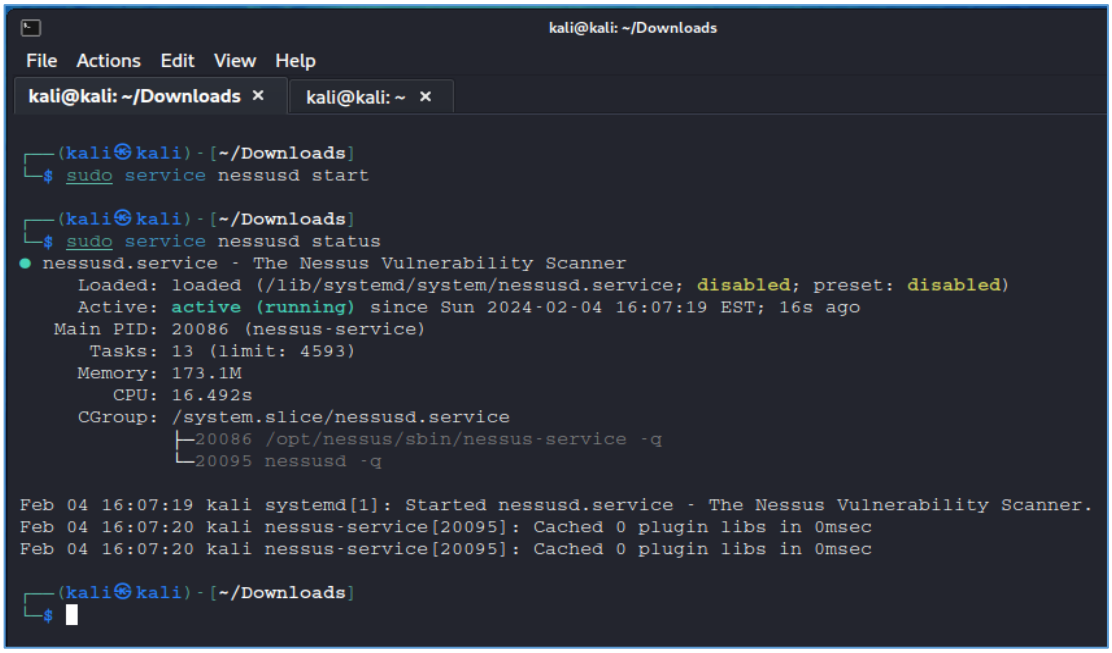
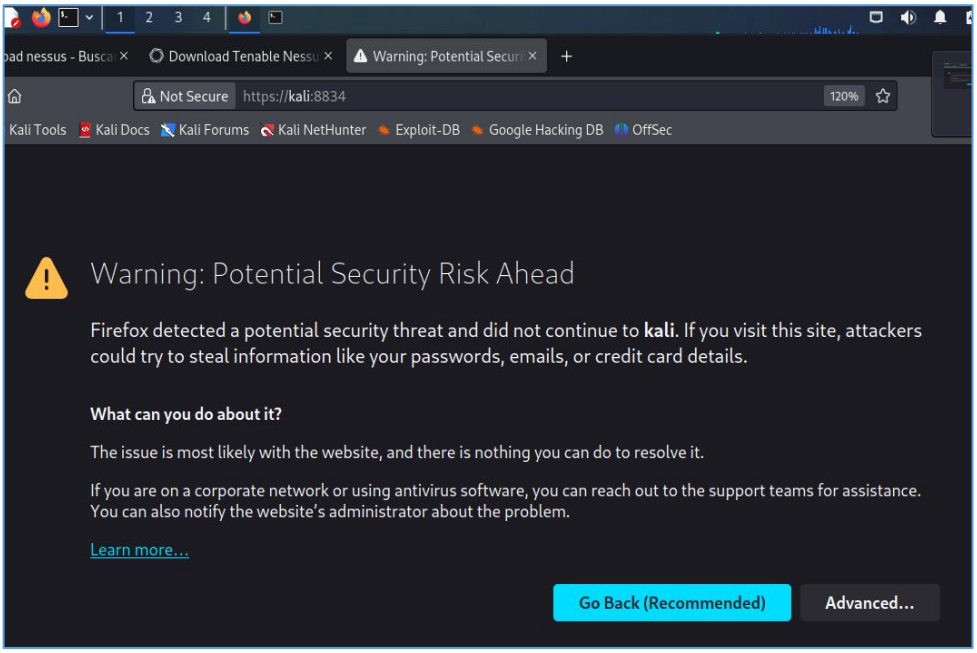
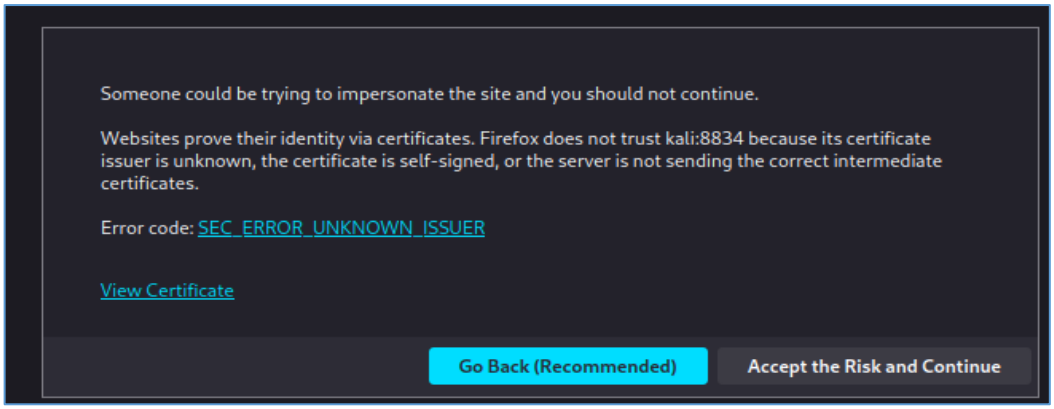


Imagen de inicialización de servicios de Nessus

Ahora nos vamos a dirigir a la dirección que se configuró para el acceso vía web de Nessus: para el ejemplo tenemos; https://kali:8834



Para poder iniciar con la parametrización de la herramienta debemos dar clic en Advanced, luego Accept the risk and continue



Nos registramos con una cuenta institucional para proceder a registrarnos:

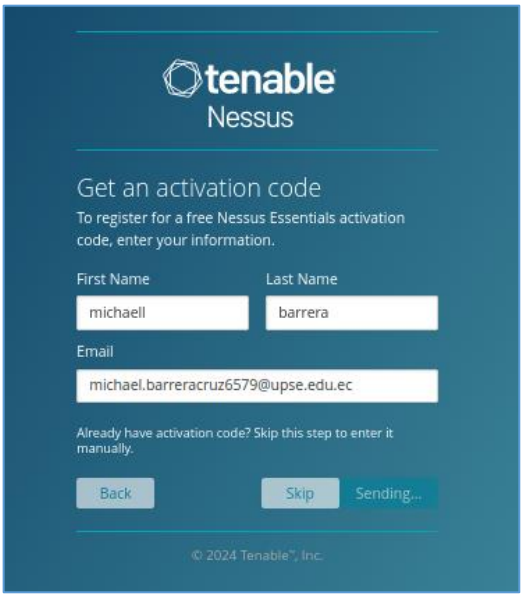


Imagen de registro de datos

A continuación, observaremos la información de la Licencia:

Activation Code: YJR4-A4LM-BQLV-GTLK-X2CJ

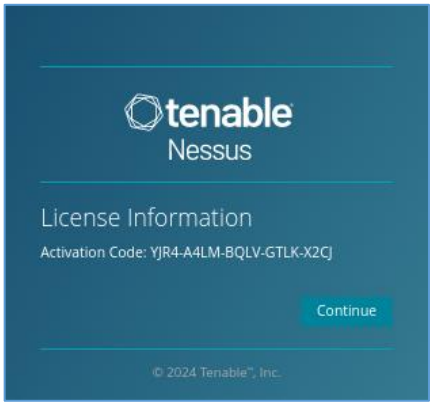


Imagen de Código de activación

Una vez aceptado y registrado la información, se procede a descargar los plugins necesarios para realizar el laboratorio con Nessus

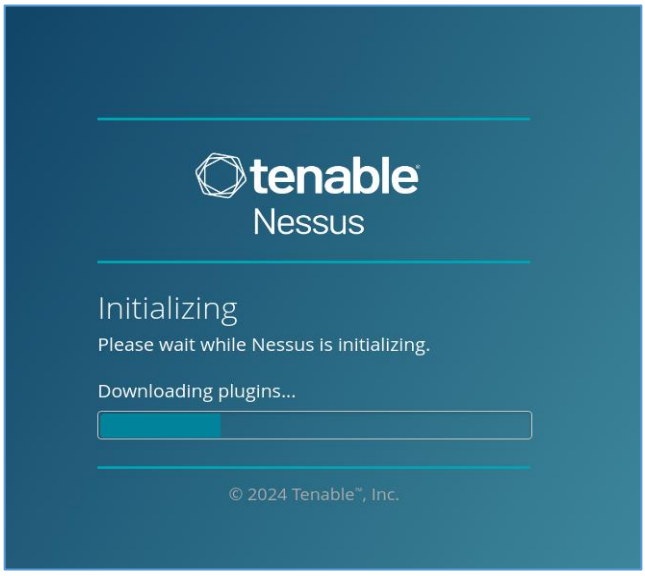


Imagen de inicialización y descarga de plugins en Nessus

Posterior a la inicialización se puede observar la descarga restante de los plugin necesarios para Nessus

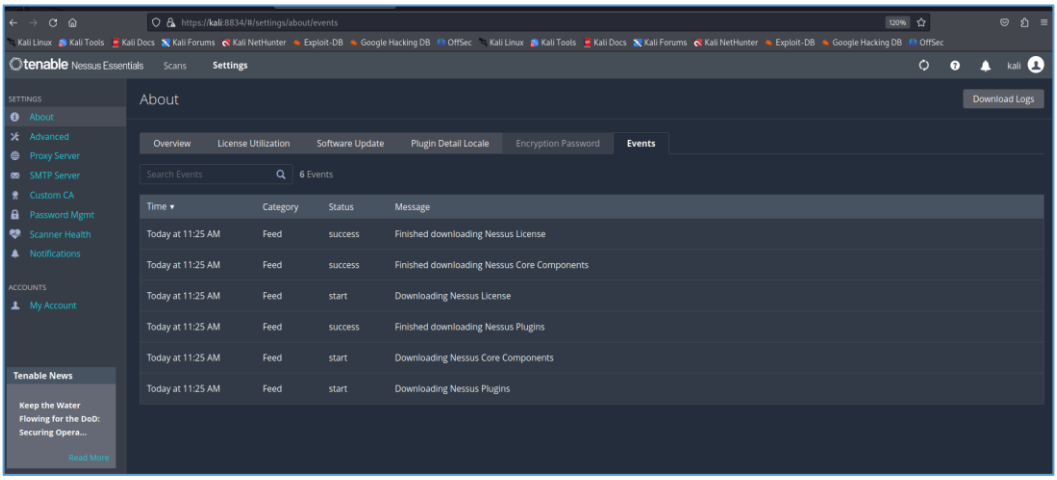
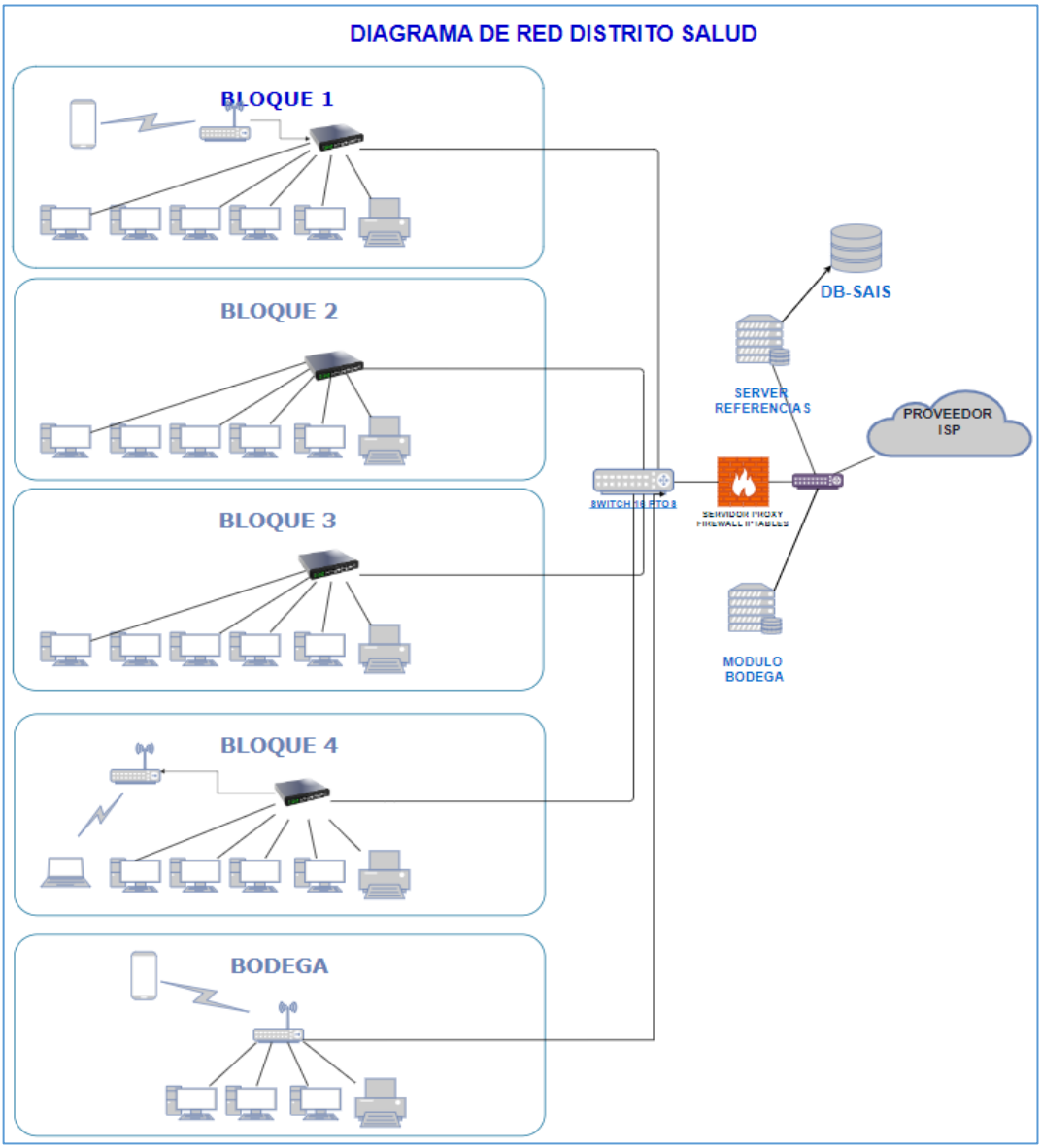
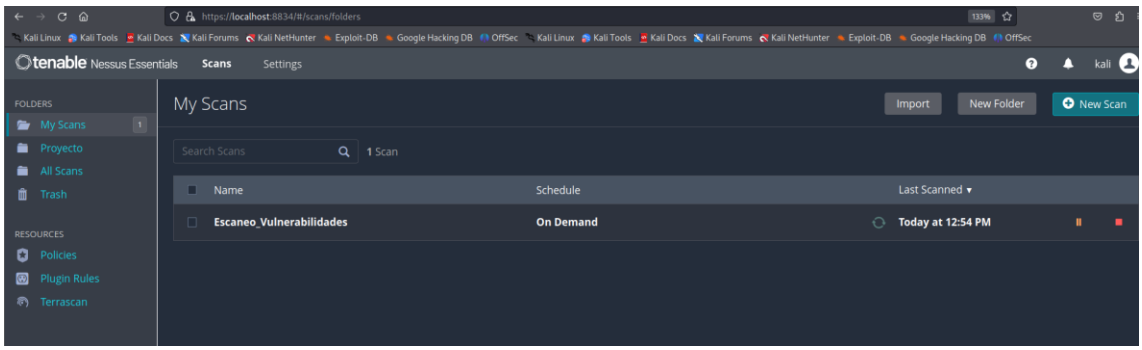


Imagen de configuración pendiente en Nessus

ANEXO 3: DIAGRAMA DE RED, ELABORADO PARA EL TRABAJO DE INVESTIGACION:



ESCANEO A SERVIDOR PROXY



ANEXO 4: INSTALACION Y CONFIGURACION DE HERRAMIENTA OPENVAS

Antes de instalar la herramienta se recomienda actualizar los repositorios de la maquina Kali para no tener inconvenientes en su instalación ni configuración:

```
$ sudo apt-get update && sudo apt-get upgrade -y
```

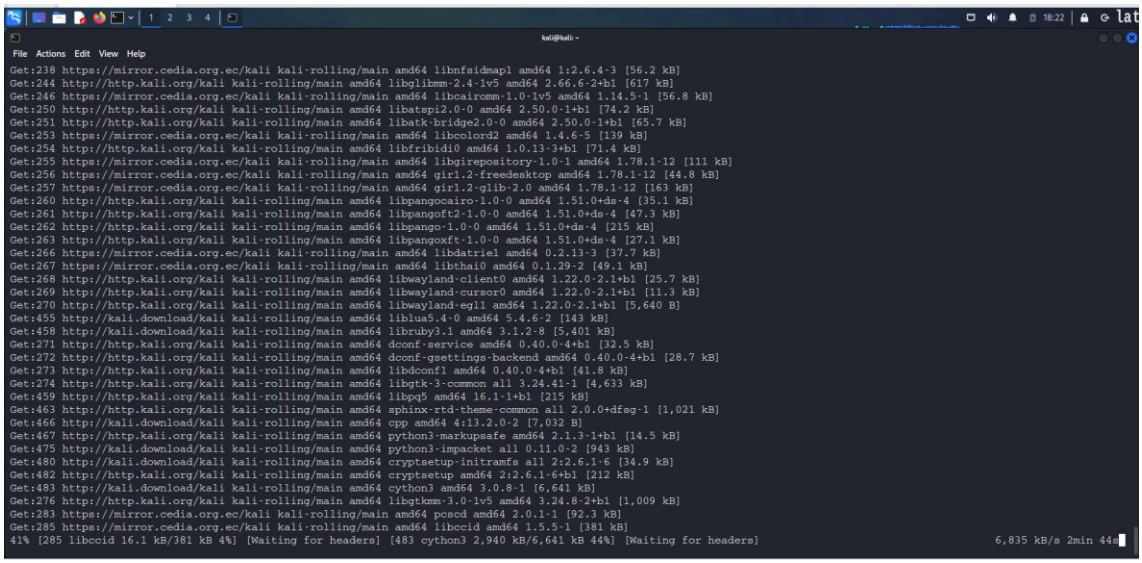
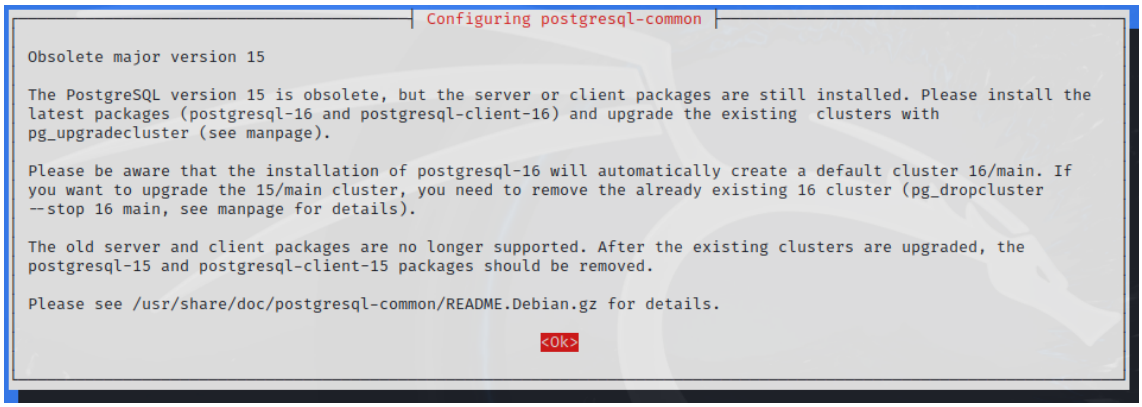
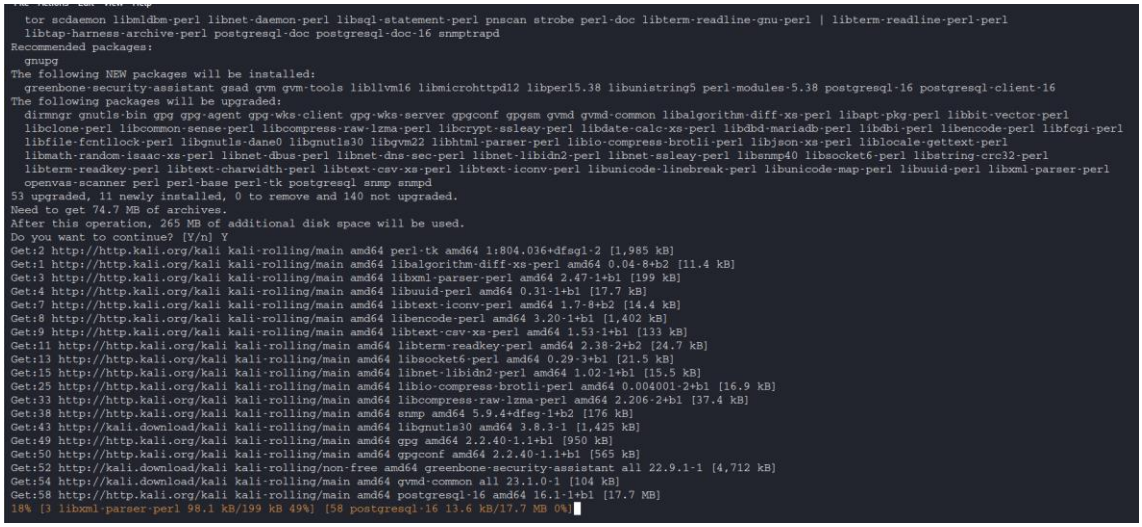


Imagen de actualización de iso Kali_linux



Una vez que se ha logrado actualizar el sistema base Kali, se procede con la instalación de la herramienta mediante el siguiente comando:

```
$ sudo apt install openvas
```



Luego de la instalación de programa OpenVAS, se debe configurar la herramienta (gestor de OpenVAS) mediante la siguiente línea:

```
$ sudo gvm-setup
```

Es probable que durante esta instalación se presenten problemas de arranque del archivo instalador, como veremos a continuación:

```
[>] Starting PostgreSQL service
[-] ERROR: The default PostgreSQL version (15) is not 16 that is required by libgvmd
[-] ERROR: libgvmd needs PostgreSQL 16 to use the port 5432
[-] ERROR: Use pg_upgradecluster to update your PostgreSQL cluster
```

Ante estos 3 errores se deberán realizar los siguientes pasos para poder solucionar y posterior continuar con la instalación del gvm-setup sin problemas.

Paso 1: digitar el siguiente comando para poder visualizar los clústers en el gestor de base de datos postgresql

$ pg_lsclusters

Ver	Cluster	Port	Status	Owner	Data directory	Log file
15	main	5432	online	postgres	/var/lib/postgresql/15/main	/var/log/postgresql/postgresql-15-main.log
16	main	5433	online	postgres	/var/lib/postgresql/16/main	/var/log/postgresql/postgresql-16-main.log

El resultado anterior muestra dos clústeres en línea escuchando en los puertos 5432 y 5433. Dado que el clúster de destino 16/principal ya existe, se debe eliminar temporalmente para evitar el error. La existencia del clúster 16/principal no significa

necesariamente que el clúster antiguo ya se haya actualizado; simplemente significa que hay un clúster para esa versión.

Paso 2: debemos actualizar el cluster de la versión 15 al 16, mediante el siguiente comando:

```
$ sudo pg_upgradecluster 15 main 16
```

Para completar la actualización, primero se debe detener y eliminar el clúster 16/principal.

Paso 3: se debe digitar la siguiente línea de comando en el terminal Kali

```
$ sudo pg_ctlcluster 16 main stop
$ sudo pg_dropcluster 16 main
```

Ahora debemos actualizar el clúster de PostgreSQL, una vez realizados los cambios denotados en los pasos anteriores:

Paso 4: digitamos la línea siguiente:

```
$ sudo pg_upgradecluster 15 main
```

Paso 5: Si no necesita el clúster PostgreSQL anterior, debe eliminarlo.

```
$ sudo pg_dropcluster 15 main
```

Ahora debemos remover los paquetes que ya no utilizaremos del Postgresql 15

Paso 6: mediante la línea siguiente:

```
$ sudo apt autoremove
```

Ahora solo debemos visualizar el único clúster de postgresql

Paso 7: para esto digitamos la siguiente línea en la terminal.

```
$ pg_lsclusters
```

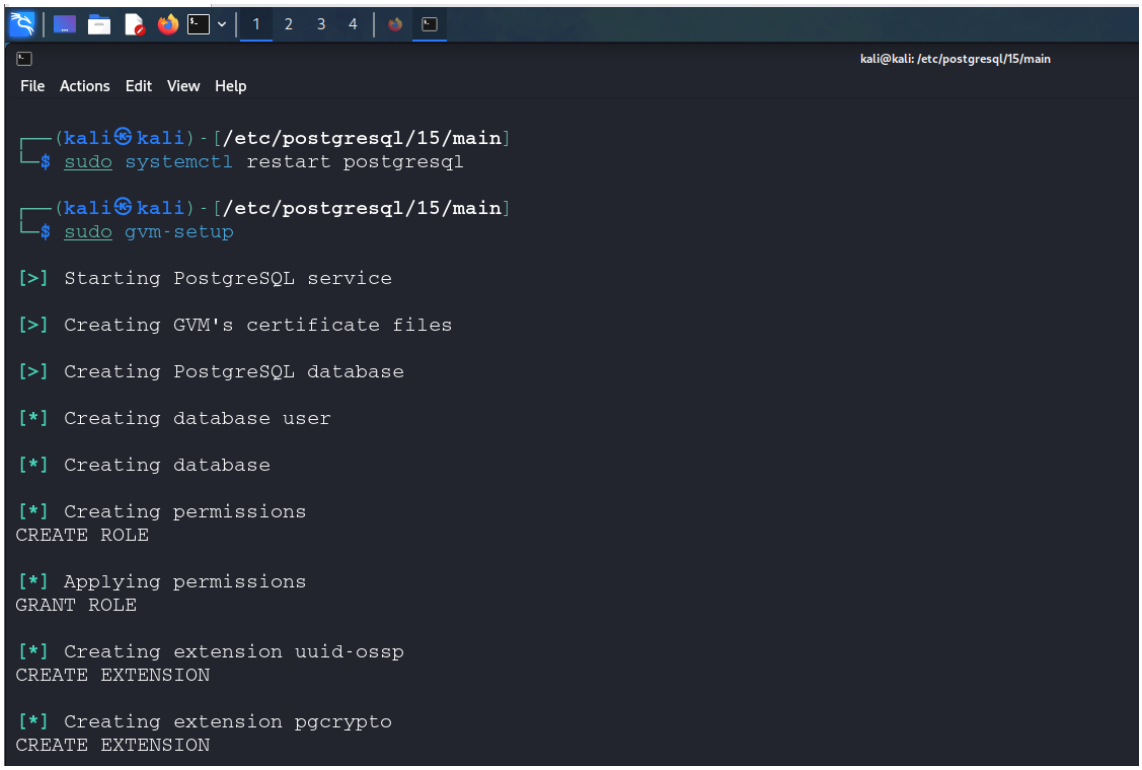
Para culminar este apartado se debe reiniciar el servicio de postrgres, con la línea:

```
$ sudo systemctl restart postgresql
```

Una vez realizado los pasos anteriores, tendremos listo todo para poder retomar la instalación como se indicará a continuación.

Ejecutamos la línea:

```
$ sudo gvm-setup
```



Una vez instalado obtendremos el siguiente resultado, donde debemos anotar el usuario por defecto (admin) y clave (genérica) para poder acceder al servicio de la herramienta greenbone-openvas vía web.

Posterior a esto, debemos iniciar el servicio de OpenVAS mediante la línea:

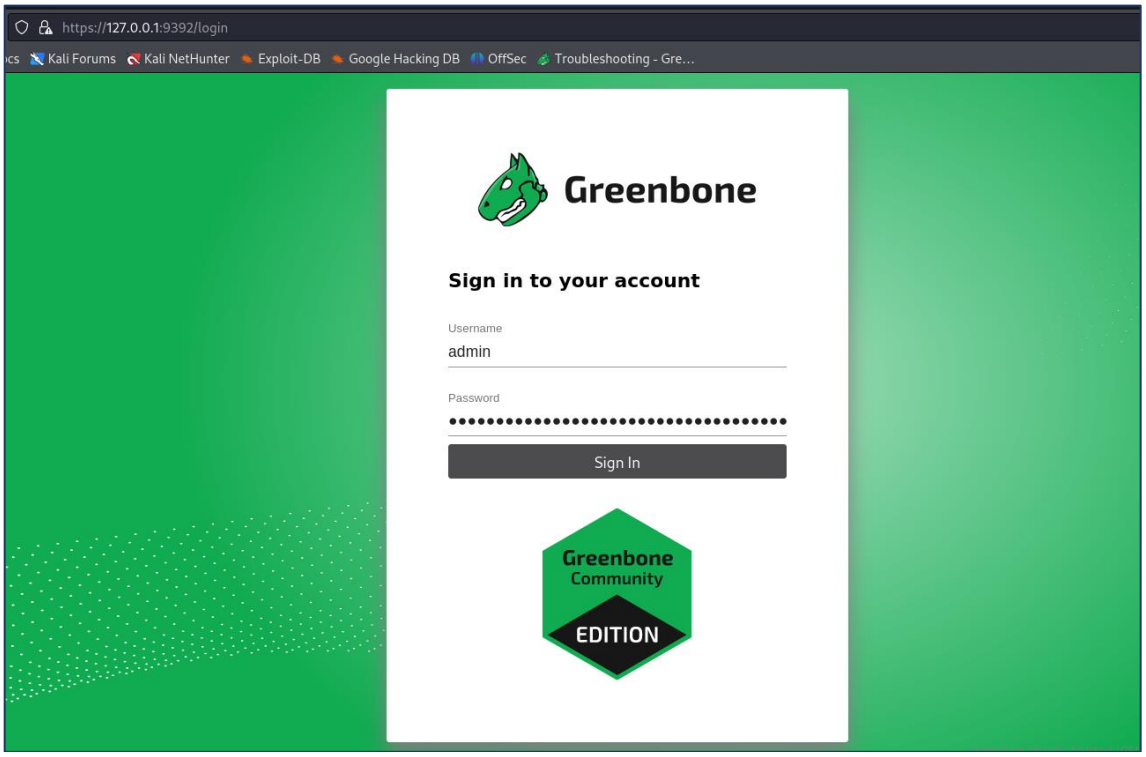
```
$ sudo gvm-start
```

```
┌──(root㉿kali)-[/etc/postgresql/15/main]
└─# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>]  Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

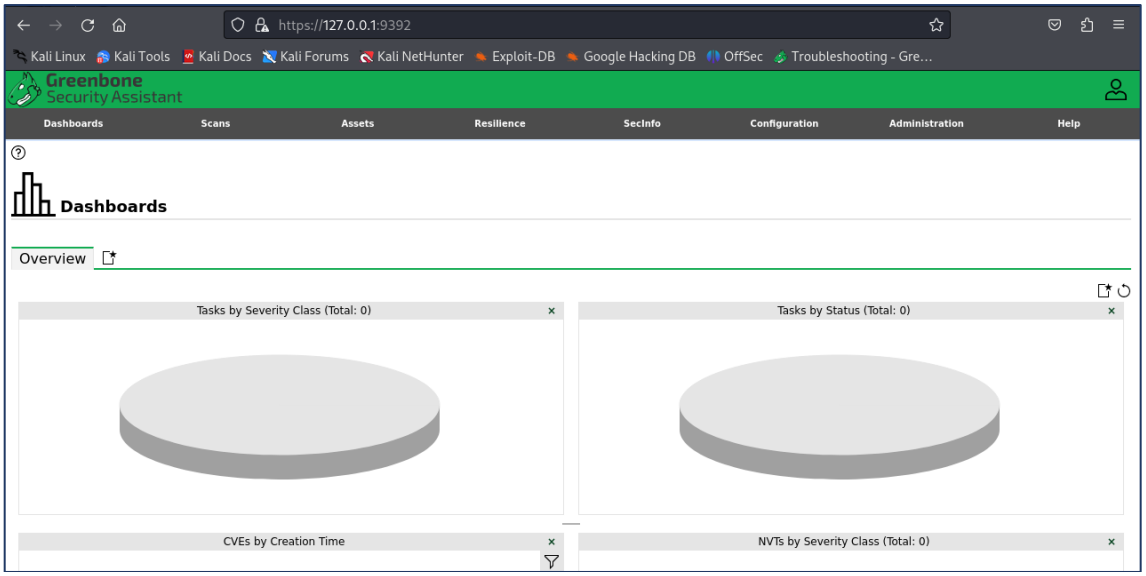
Como podemos observar la página que se configura es:

https://127.0.0.1:9392

Si no redirige de forma automática a la página web, podemos digitar la dirección antes mencionada en un nuevo navegador, para garantizar que la herramienta funcione sin problemas.

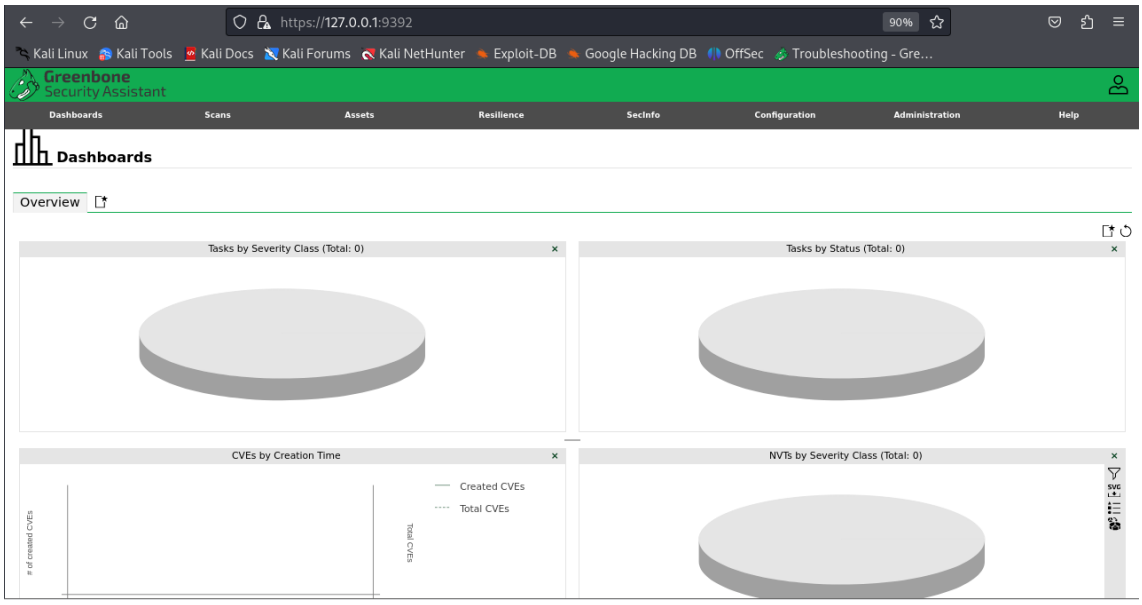


Una vez colocado las credenciales de acceso, previamente establecidas por la herramienta, presionamos en el botón Sign In



Como se observa en la imagen anterior, carga la herramienta sin resultados, todo en blanco, lo que denota la falta de paquetería adicional, para lo cual se debe digitar 3 lineas de comandos

En esta ventana visualizamos que ya tenemos nuestra herramienta instalada, sin embargo, hace falta la actualización de los paquetes con las q trabaja Open Vas.



Por lo que debemos realizar esa parte mediante los siguientes comandos:

Ante de empezar con este proceso se debe paralizar la ejecución de la herramienta:

```
$ sudo gvm-stop
```

Luego se procede a ejecutar las siguientes líneas:

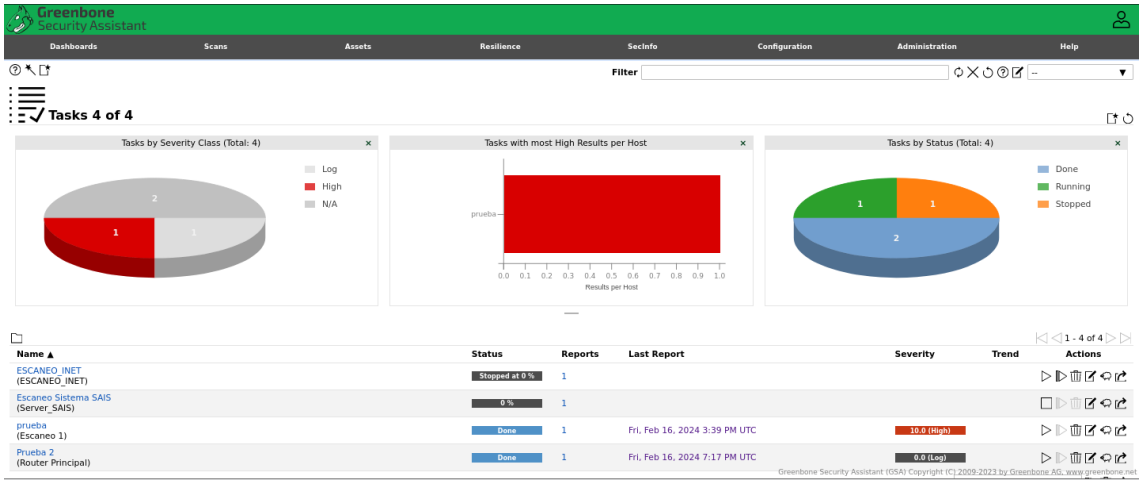
```
$ sudo greenbone-feed-sync --type GVMD_DATA
```

```
$ sudo greenbone-feed-sync --type SCAP
```

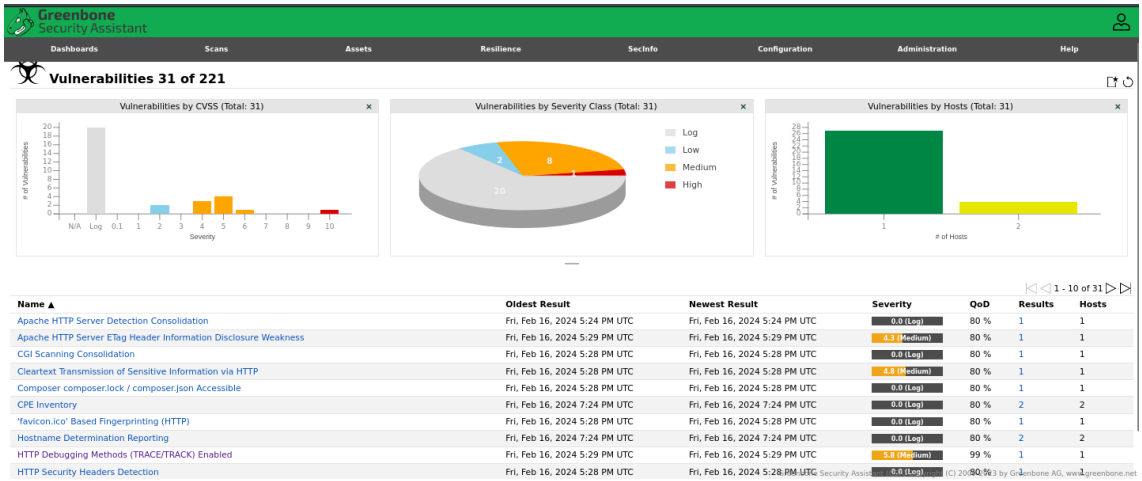
```
$ sudo greenbone-feed-sync --type CERT
```

Ahora para ejecutar la herramienta debemos digitar la siguiente línea en el terminal:

```
$ sudo gvm-start
```



Visualización de Vulnerabilidades:

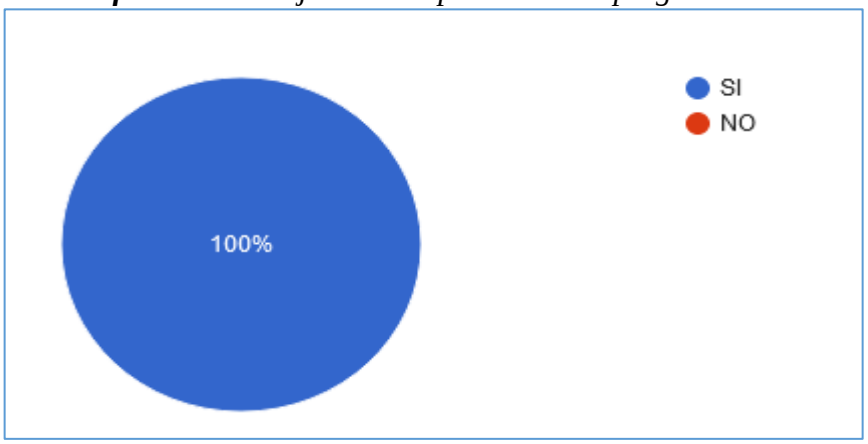


ANEXO 5: Encuesta realizada a personal de tecnologías del distrito de salud

https://forms.gle/a5rhxqVjoaHkH6z67

1. **¿El área en la que desempeña sus labores tiene una política formal de seguridad de la información?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 1*

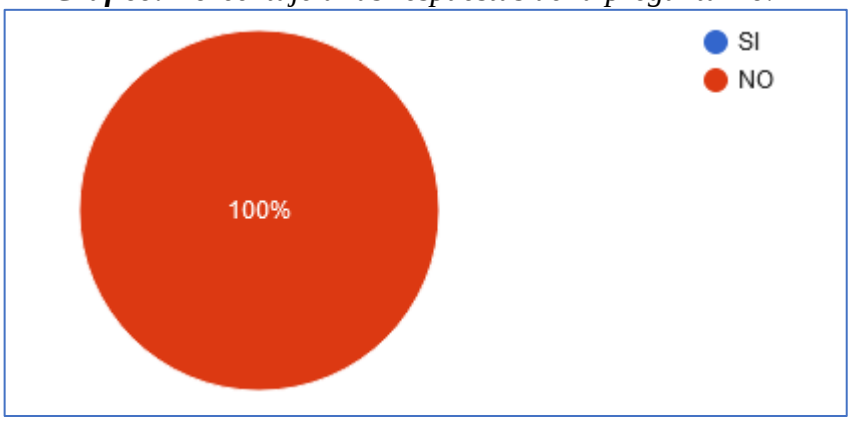


Fuente*: trabajo de investigación, elaboración propia*

ANALISIS: Mediante la encuesta realizada se verificó que el 100% de los funcionarios indican que NO se cuenta con una política formal de seguridad de la información.

2. **¿Realizan evaluaciones periódicas de vulnerabilidades en su infraestructura de red?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 2*

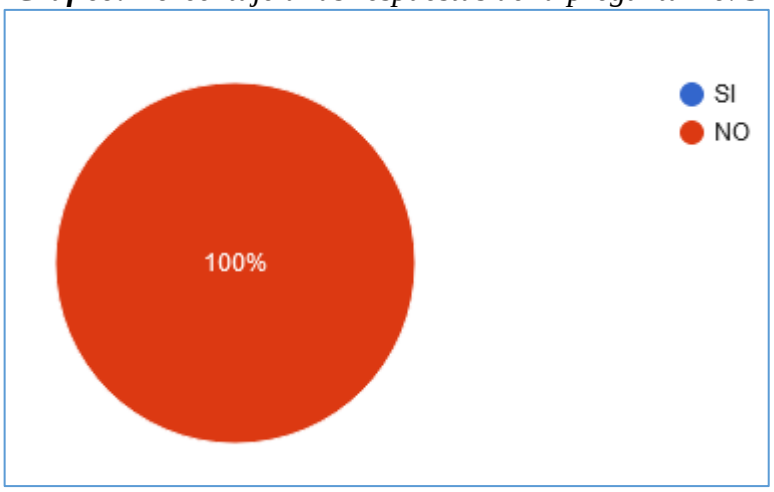


Fuente*: trabajo de investigación, elaboración propia*

ANALISIS: Durante la encuesta realizada se obtuvo que el 100% de los funcionarios indican que NO se realizan evaluaciones de vulnerabilidades en su infraestructura del Distrito de Salud.

3. **¿Utilizan herramientas para monitorear la seguridad de su infraestructura de red?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 3*

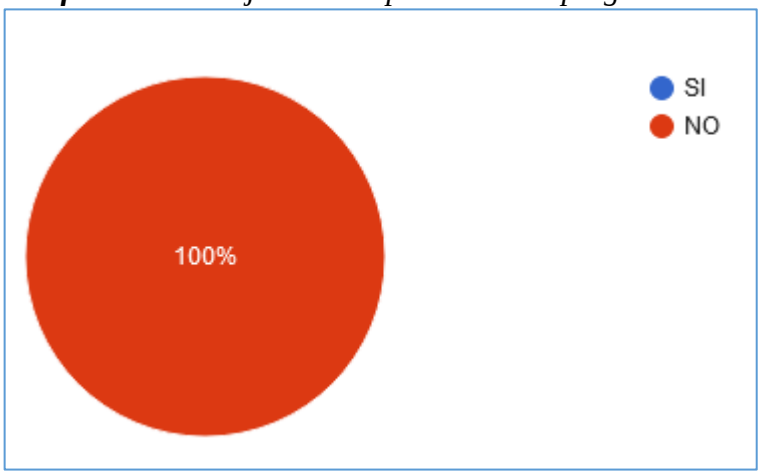


Fuente*: trabajo de investigación, elaboración propia*

ANALISIS: Mediante la encuesta realizada se obtuvo que el 100% de los funcionarios mencionan que NO utilizan herramientas para monitorear la seguridad en la infraestructura de red del Distrito de Salud.

4. **¿Cuentan con un equipo dedicado a la gestión de la seguridad de la información?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 4*

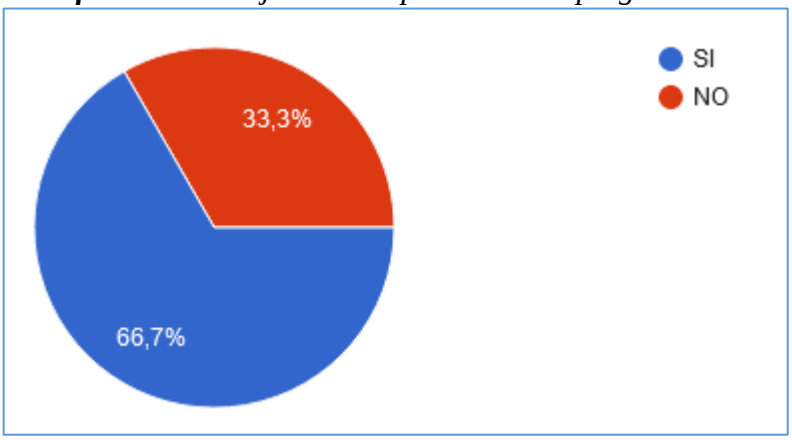


Fuente*: trabajo de investigación, elaboración propia*

ANALISIS: Mediante la encuesta realizada se logró recabar la siguiente información: que el 100% de los funcionarios mencionan que NO existe un equipo dedicado para la gestión de la seguridad de la información del Distrito de Salud.

5. **¿Han experimentado incidentes de seguridad en algún momento?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 5*

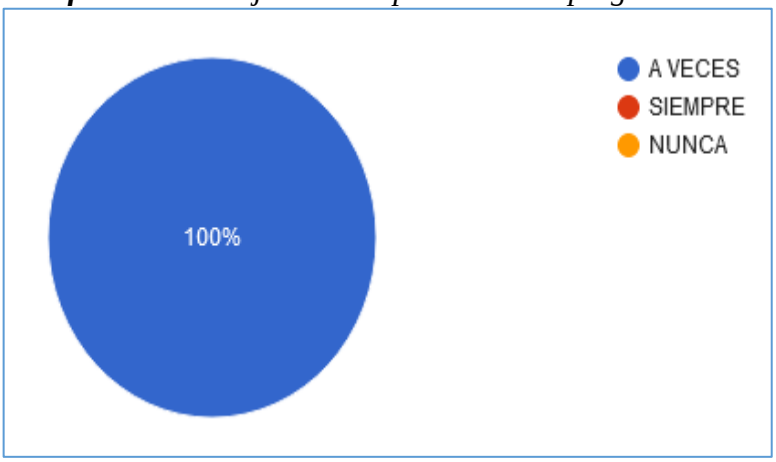


Fuente*: trabajo de investigación, elaboración propia*

ANALISIS: Durante la encuesta realizada se logró recabar la siguiente información: que el 66.7% de los funcionarios mencionan que si han experimentado incidentes de seguridad para la gestión de la infraestructura del Distrito de Salud.

6. **¿Realizan copias de seguridad de forma regular?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 6*

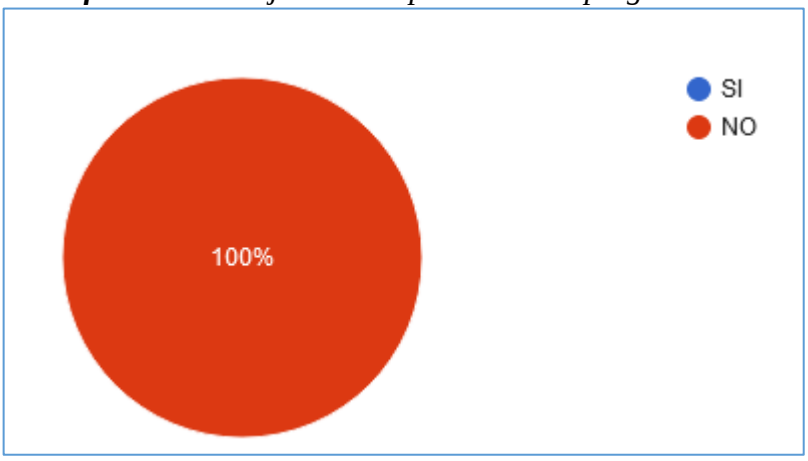


Fuente*: trabajo de investigación, elaboración propia*

ANÁLISIS: Mediante la encuesta realizada se logró recabar la siguiente información: que el 100% de los funcionarios de TI mencionan que NO se realizan copias de seguridad de forma regular, de la información que existe en los equipos dentro de la infraestructura de red del Distrito de Salud.

7. **¿Tienen un plan de respuesta ante incidentes de seguridad?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 7*

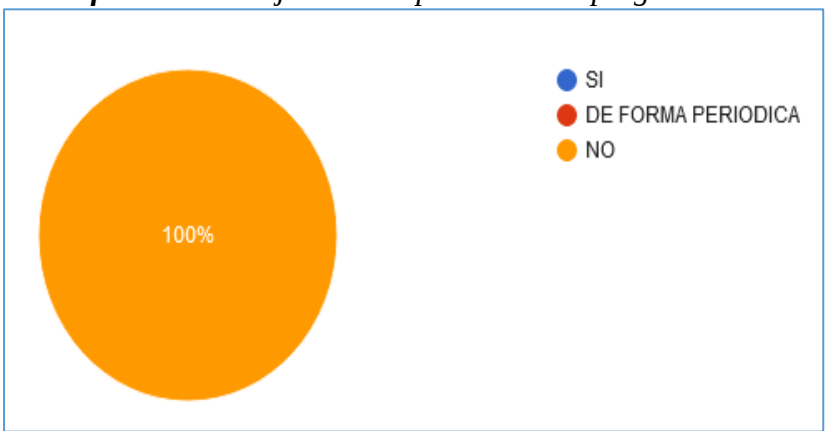


Fuente*: trabajo de investigación, elaboración propia*

ANALISIS: Durante la encuesta realizada se logró receptar la siguiente información: que el 100% de los funcionarios mencionan que NO cuentan con un plan de respuesta ante alguna incidencia de ciberseguridad que se pueda presentar.

8. **¿Ofrecen capacitación en seguridad de la información a sus compañeros?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 8*

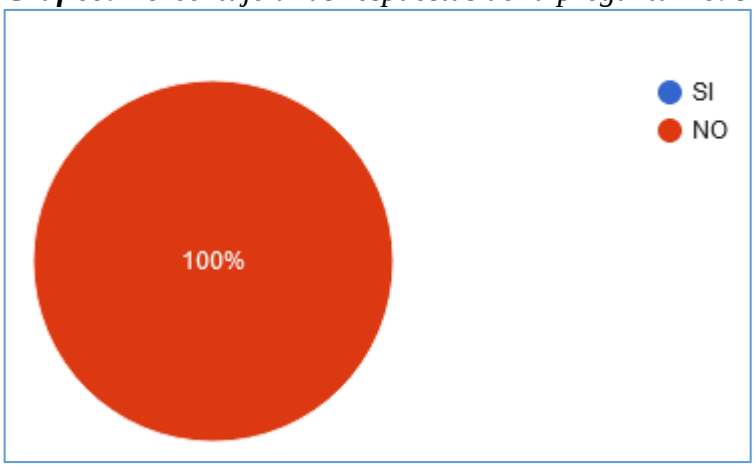


Fuente*: trabajo de investigación, elaboración propia*

ANÁLISIS: Mediante la encuesta realizada se logró recabar la siguiente información: que el 100% de los funcionarios de TI mencionan que NO se brindan capacitaciones a los colaboradores de la institución, como parte de una estrategia hacia la mejora de la seguridad dentro de la entidad.

9. **¿Utilizan algún estándar o marco de seguridad reconocido, como ISO 27001?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 9*



Fuente*: trabajo de investigación, elaboración propia*

ANÁLISIS: Durante la encuesta realizada se logró recabar la siguiente información: que el 100% de los funcionarios indican que NO utilizan estándar alguno para que de una u otra forma mitigar las vulnerabilidades existentes.

10. **¿Qué medidas adicionales han implementado debido a la pandemia de COVID-19 para garantizar la seguridad de la información?**

Gráfico: *Porcentaje a las respuestas de la pregunta No. 10*

Fuente*: trabajo de investigación, elaboración propia*

ANÁLISIS: Mediante la encuesta realizada se logró recabar la siguiente información: que el 100% de los funcionarios mencionan que NO se han

implementado medidas adicionales postpandemia, una vez que, de acuerdo con lo mencionado en la introducción del trabajo de investigación, los ataques informáticos han venido en aumento, sobre todo para la época de pandemia ya citado.

ANEXO 6: GUIA BÁSICA PARA IMPLEMENTACION DE ISO 27001: 2022

La norma ISO/IEC 27001:2022 proporciona un marco integral para la gestión de la seguridad de la información en una organización. Implementar un plan de seguridad basado en esta norma ayuda a proteger la infraestructura de red de amenazas y vulnerabilidades.

A continuación, se destacan los ítems para el diseño:

1. Evaluación de riesgos:

Identificar activos: Determinar los activos de información críticos (datos, software, hardware, etc.) dentro de la red.

Analizar amenazas y vulnerabilidades: Identificar las amenazas potenciales (ataques cibernéticos, errores humanos, desastres naturales) y las vulnerabilidades existentes en la infraestructura.

Evaluar el impacto: Determinar el impacto potencial de cada amenaza en los activos de información.

2. Controles de seguridad:

Implementar controles: Seleccionar e implementar los controles de seguridad adecuados de la norma ISO/IEC 27001:2022 para mitigar los riesgos identificados.

Priorizar controles: Enfocarse en los controles más relevantes para los activos de información críticos y los riesgos más altos.

Personalizar controles: Adaptar los controles a las necesidades específicas de la organización y la infraestructura de red.

3. Gestión y mejora:

Establecer políticas: Documentar las políticas de seguridad que definen el enfoque de la organización para la seguridad de la información.

Capacitar al personal: Brindar capacitación al personal sobre las políticas de seguridad, los procedimientos y sus responsabilidades.

Monitorear y revisar: Monitorear y revisar continuamente la eficacia del plan de seguridad y realizar las actualizaciones necesarias.

Mejores prácticas:

Enfoque proactivo: Anticiparse a las amenazas emergentes y actualizar el plan de seguridad en consecuencia.

Cultura de seguridad: Fomentar una cultura de seguridad dentro de la organización donde todos los empleados comprendan la importancia de la protección de la información.

Comunicación efectiva: Asegurar una comunicación clara y regular sobre la seguridad de la información a todos los niveles de la organización.

Consideraciones adicionales:

Marco legal y regulatorio: Cumplir con las leyes y regulaciones aplicables a la seguridad de la información, sin dejar a un lado la Ley de Protección de Datos Personales.

Tecnologías nuevas: Mantenerse actualizado sobre las nuevas tecnologías y su impacto en la seguridad de la red.

ANEXO 7: GUÍA PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

1. Controles organizacionales

1.1. Políticas de seguridad de la información

1.2. Roles y responsabilidades de seguridad de la información

1.3. Separación de funciones

1.4. Responsabilidades de la dirección

1.5. Contacto con las autoridades

1.6. Contacto con grupos de interés especial

1.7. Inteligencia de amenazas

1.8. Seguridad de la información en la Gestión de proyectos

1.9. Inventario de información y otros activos asociados

1.10. Uso aceptable de la información y otros activos asociados

1.11. Devolución de activos

1.12. Clasificación de la información

1.13. Etiquetado de la información

1.14. Transferencia de información

1.15. Control de acceso

1.16. Gestión de identidad

1.17. Información de autenticación

1.18. Derechos de acceso

1.19. Seguridad de la información en las relaciones con proveedores

1.20. Abordar la seguridad de la información en los acuerdos con proveedores

1.21. Gestión de seguridad de la información en la cadena de suministro de las TIC

1.22. Monitoreo, revisión y gestión de cambios de servicios de proveedores

1.23. Seguridad de la información para el uso de servicios en la nube

1.24. Planificación y preparación de la gestión de incidentes de seguridad de la información

1.25. Evaluación y decisión sobre eventos de seguridad de la información

1.26. Respuesta a incidentes de seguridad de la información

1.27. Aprendiendo de los incidentes de seguridad de la información

1.28. Recopilación de evidencias

1.29. Seguridad de la información durante la interrupción

1.30. Preparación de las TIC para la continuidad del negocio

1.31. Requisitos legales, estatutarios, reglamentarios y contractuales

1.32. Derechos de propiedad intelectual

1.33. Protección de registros

1.34. Privacidad y protección de PII

1.35. Revisión independiente de seguridad de la información

1.36. Cumplimiento de políticas, reglas y normas de seguridad de la información

1.37. Procedimientos documentados operativos

2. Control de personas

2.1. Selección

2.2. Términos y condiciones de empleo

2.3. Concienciación, educación y formación en seguridad de la información

2.4. Proceso disciplinario

2.5. Responsabilidades después de la terminación o cambio de empleo

2.6. Acuerdos de confidencialidad o no divulgación

2.7. Trabajo remoto

2.8. Reporte de eventos de seguridad de la información

3. Controles físicos

3.1. Perímetros de seguridad física

3.2. Entrada física

3.3. Seguridad de oficinas, despachos e instalaciones

3.4. Monitoreo de seguridad física

3.5. Protección contra las amenazas externas y ambientales

3.6. Trabajo en áreas seguras

3.7. Puesto de trabajo despejado y pantalla limpia

3.8. Ubicación y protección de equipos

3.9. Seguridad de los activos fuera de las instalaciones

3.10. Medios de almacenamiento

3.11. Servicios de soporte

3.12. Seguridad del cableado

3.13. Mantenimiento de equipo

3.14. Eliminación segura o reutilización de equipos

4. Controles tecnológicos

4.1. Dispositivos de usuario final

4.2. Derechos de acceso privilegiado

4.3. Restricción de acceso a la información

4.4. Acceso al código fuente

4.5. Autenticación segura

4.6. Gestión de la capacidad

4.7. Protección contra malware

4.8. Gestión de vulnerabilidades técnicas

4.9. Gestión de la configuración

4.10. Eliminación de información

4.11. Enmascaramiento de datos

4.12. Prevención de fuga de datos

4.13. Copia de seguridad de la información

4.14. Redundancia de las instalaciones de tratamiento de información

4.15. Registro de eventos

4.16. Actividades de monitoreo

4.17. Sincronización del reloj

4.18. Uso de programas de utilidad privilegiados

4.19. Instalación de software en sistemas operativos

4.20. Seguridad de redes

4.21. Seguridad de los servicios de red

4.22. Separación en las redes

4.23. Filtrado web

4.24. Uso de criptografía

4.25. Ciclo de vida de desarrollo seguro

4.26. Requisitos de seguridad de la aplicación

4.27. Arquitectura del sistema seguro y principios de ingeniería

4.28. Codificación segura

4.29. Pruebas de seguridad en el desarrollo y la aceptación

4.30. Desarrollo subcontratado

4.31. Separación de los entornos de desarrollo, prueba y producción

4.32. Gestión de cambios

4.33. Información de prueba

4.34. Protección de los sistemas de información durante las pruebas de auditoría