UNIVERSIDAD TÉCNICA DE AMBATO

CENTRO DE POSGRADOS

PROGRAMA DE MAESTRÌA EN TECNOLOGÌAS DE LA INFORMACIÓN

COHORTE 2022

Tema: PROCEDIMIENTO PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA PERIMETRAL EN LA INFRAESTRUCTURA DE UNA ORGANIZACIÓN.

Trabajo de Titulación, previo a la obtención del Título de Cuarto Nivel de Magíster en Tecnologías de la Información Mención Seguridad de Redes y Comunicaciones

Modalidad del Trabajo de Titulación: Componente de Investigación Aplicada y de Desarrollo.

Autor: Ingeniero Hugo David Peña Rosillo

Director: Ingeniero Víctor Santiago Manzano Villafuerte**,** Magister

Ambato – Ecuador

2023

A la Unidad Académica de Titulación del Centro de Posgrados

El Tribunal receptor del Trabajo de Titulación, presidido por el Ingeniero Oscar Fernando Ibarra Torres Magister, Delegado por el Ingeniero Héctor Fernando Gómez Alvarado PhD, Director del Centro de Posgrados e integrado por los señores: *Ingeniera María José Bravo Ramos PhD e Ingeniero José Miguel Ocaña Chiluisa PhD,* designados por la Unidad Académica de Titulación del Centro de Posgrados de la Universidad Técnica de Ambato, para receptar el Trabajo de Titulación con el tema: "*Procedimiento para la gestión de la seguridad informática perimetral en la infraestructura de una organización",* elaborado y presentado por el señor Ingeniero Hugo David Peña Rosillo para optar por el Titulo de cuarto nivel de Magíster en Tecnologías de la Información mención Seguridad de Redes y Comunicaciones; una vez escuchada la defensa oral del Trabajo de Titulación, el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing.Oscar Fernando Ibarra Torres Mgtr.
Presidente y Miembro del Tribunal

Ing. María José Bravo Ramos PhD.
Miembro del Tribunal

Ing. José Miguel Ocaña Chiluisa PhD.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE TITULACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Titulación presentado con el tema: Procedimiento para la gestión de la seguridad informática perimetral en la Infraestructura de una Organización, le corresponde exclusivamente a: Ingeniero Hugo David Peña Rosillo, Autor bajo la Dirección de Ingeniero Víctor Santiago Manzano Villafuerte Magister, Director del Trabajo de Titulación, y el patrimonio intelectual a la Universidad Técnica de Ambato.

Ingeniero Hugo David Peña Rosillo
c.c.: 0202048070
AUTOR

Ingeniero Víctor Santiago Manzano Villafuerte, Magister
c.c.: 1803364627
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Titulación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de este, dentro de las regulaciones de la Universidad.

Ingeniero Hugo David Peña Rosillo
c.c.: 0202048070

INDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

AGRADECIMIENTO

A Dios por ser mi ángel protector, brindarme fortaleza, sabiduría y bendecir cada paso de mi vida.

A la Universidad Técnica de Ambato por permitirme continuar con mi formación académica.

Al personal docente de la Maestría en Tecnologías de la Información por los conocimientos impartidos con su empeño y dedicación.

De manera especial a mi tutor de tesis el Ing. Santiago Manzano, por su tiempo, apoyo y asesoramiento para el desarrollo del proyecto de investigación.

Al "Hospital Alfredo Noboa Montenegro", por su apertura para el desarrollo del trabajo de investigación, al Ing. Raúl Camacho y Ing. Wilmer Quicaliquin por su colaboración.

Hugo David Peña Rosillo

DEDICATORIA

A Dios, al Divino Niño por ser la luz que guía mi camino.

A mis padres Mercedes y Hugo por ser un apoyo incondicional y demostrarme que con dedicación todo es posible.

A mis hermanos Melissa y Anthony.

A mi abuelita Flor y mi tía Laurita, que sin importar las circunstancias y la distancia han estado a mi lado apoyándome.

Hugo David Peña Rosillo

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
MAESTRÍA EN TECNOLOGIAS DE LA INFORMACIÓN
COHORTE 2022

TEMA:

PROCEDIMIENTO PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA PERIMETRAL EN LA INFRAESTRUCTURA DE UNA ORGANIZACIÓN.

MODALIDAD DE TITULACIÓN: *Proyecto de Titulación con Componente de Investigación Aplicada y de desarrollo.*
AUTOR: *Ingeniero Hugo David Peña Rosillo*
DIRECTOR: *Ingeniero Víctor Santiago Manzano Villafuerte Magister*
FECHA: *Veinte y siete de noviembre de dos mil veinte y tres.*

RESUMEN EJECUTIVO

En la actualidad, uno de los principales problemas a nivel mundial es la seguridad informática a la que están expuestos los sistemas TI, debido ataques informáticos que pueden causar daños a su infraestructura, comprometiendo la integridad y confidencialidad de su información.

El trabajo de investigación titulado "Procedimiento para la gestión de la seguridad informática perimetral en la infraestructura de una organización" es un estudio que se basa en mejorar y mantener actualizado los procesos de seguridad perimetral en el "Hospital General Alfredo Noboa Montenegro" partiendo de un modelo de gestión de seguridad en base a Normas Internacionales que permitan el control y manejo de datos con total integridad.

El estudio se desarrolló en base a un enfoque cuantitativo y cualitativo, donde se utilizó instrumentos como la entrevista, dirigidos a los involucrados del área de TI con el objetivo de conocer la situación actual de la institución en el campo de seguridad, que amenazas y vulnerabilidades ha presentado su sistema y cuál ha sido su reacción de respuesta antes estos eventos e incidentes. Para la recolección de datos se aplicó el método interpretativo basándose en un análisis de semejanzas de conceptos de los datos obtenidos.

El objetivo final del proyecto, se consideró un análisis de la familia de la Norma ISO/IEC 27001, en los que se refiere a políticas de seguridad informática, políticas de protección de datos, realizar un análisis de activos y tratamiento de riesgos utilizando la metodología de MAGERIT, mediante criterios de valoración para el cálculo de la probabilidad de ocurrencia, evaluación de impacto y riesgos, con la finalidad de establecer mecanismos de control para mitigar los riesgos de amenazas y vulnerabilidades que pongan en peligro la seguridad informática de la institución, el procedimiento de gestión de seguridad informática perimetral busca crear una cultura de seguridad en la institución.

DESCRIPTORES: *NORMATIVA, SEGURIDAD INFORMÁTICA, POLITICAS, INFRAESTRUCTURA, INTEGRIDAD, PROTECCION DE DATOS.*

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Introducción.

A nivel mundial, la conectividad y acceso a las redes ha tenido un desarrollo global principalmente en lo que se refiere a la transformación de la infraestructura tecnológica, tomando principalmente como punto relevante la penetración e interacción de dispositivos internos y externos , se prevé que para el año 2028 los ataques informáticos sean más letales en donde los ciberataques, ciberdelincuentes utilicen nuevas técnicas e inteligencia artificial al momento de vulnerar los sistemas de una infraestructura de red empresarial u organizacional, sean estas por medio de transmisión alámbricas o inalámbricas, accesos no autorizados y nuevos ataques informáticos.

En el país uno de los grandes problemas que enfrentan las organizaciones son las vulnerabilidades informáticas a las que pueden estar expuestas su infraestructura de red en la ejecución de sus actividades diarias, infecciones o ataques que se debe prevenir, combatir mediante la ejecución de normas, políticas y estándares de seguridad informática,

Debido a la transmisión de datos que se envía y comparte por internet con diferentes usuarios, empresas u organizaciones, la seguridad informática en momentos se ha vuelto vulnerable debido a que existen nuevos tipos de ataques informáticos, tales como, malware, ransomware, virus, gusanos, troyanos, phishing, pharming, entre otros y especialmente atacantes de sombrero negro que cuentan con mayores conocimientos especializados en el área informática.

Por tal motivo las empresas buscan elegir un modelo de gestión para garantizar la seguridad informática (SI), con la aplicación de buenas prácticas y normas recomendadas a partir de políticas y roles definidos que permitan obtener los tres pilares de la SI, es decir, la integridad, disponibilidad y confidencialidad.

El estudio de investigación tiene como objetivo realizar un procedimiento para la gestión de la seguridad informática en la infraestructura del “Hospital General Alfredo Noboa Montenegro” en base al funcionamiento y situación actual de la estructura de red, recursos y servicio informáticos importantes de la organización.

Este documento obedece a la siguiente estructura:

Capítulo I: Aborda la introducción, justificación, objetivos generales y específicos que permitan el desarrollo del estudio de investigación.

Capítulo II: se desarrolló el marco teórico, antecedentes investigativos, conceptos, normas, políticas y definiciones relacionadas con las variables en estudio.

Capítulo III: se planteó la metodología, enfoque, situación actual, así como la investigación a implementar en base a un análisis de las normas, políticas y estándares relacionados con seguridad informática,

Capítulo IV: se encuentra el análisis y resultados encontrados en el estudio de investigación

Capítulo V: se detalló las conclusiones y recomendaciones a las que llegaron el análisis.

Capítulo VI: Desarrollo del Procedimiento para le gestión de la seguridad informática perimetral en el “Hospital General Alfredo Noboa Montenegro”.

1.2. Justificación

La seguridad informática es importante en la infraestructura de red de una empresa u organización, ya que permite proteger la información en base a los recursos informáticos que conforman la red de datos de la empresa y la respuesta que estos pueden tener ante posibles riesgos y amenazas, que puedan ocasionar daños mal funcionamientos de sus recursos tecnológicos.

Según la empresa ESET se realizó un análisis a nivel de Latinoamérica sobre la seguridad de la información, estudio que se realizó en el año 2017 con el objetivo de recopilar información a los trabajadores de casi 2500 empresas obteniendo datos importantes en el campo de la seguridad. Entre las primeras se encuentran la infección de un ransomware con un 57%, seguido de las vulnerabilidades que cuenta su empresa con un 55% y 53%, reflejando un alto porcentaje para lo posible difusión del malware en sus recursos informáticos (Romero,2018).

Varias empresas locales e internacionales se han visto en serios problemas por infecciones ocasionados por virus, gusanos y malware informático que ha puesto en peligro su infraestructura de red. Según ESET, a nivel de Latinoamérica en el año 2017 se notificó 14700 vulnerabilidades, determinando que el país con mayor infección de malware y ransomware es Ecuador con 22%, mientras que Perú cuenta con un 18%, además llegando a una conclusión que a nivel de Latinoamérica solo el 25% cuentan con una política de seguridad y el 1% con posibilidad de actualizar su tecnología de seguridad (Romero,2018).

Un estudio realizado por la Policía Nacional del Ecuador y su grupo especial Interpol, detecto en base a su centro de incidentes informático y apoyado por distintas entidades de América latina determino que, el 85% de ataques a los programas informáticos son causados por error del usuario, 58% de personas dejan sus equipos tecnológicos en lugares inseguros y propensos a robos, 60% establece la misma contraseña en sus equipos tecnológicos, tarjetas de débito y crédito, 35% ha ingresado a link maliciosos enviados mediante correo electrónico, 59% hace uso del almacenamiento de información en la nube y el 80% sufre de intimidaciones en las redes sociales" (Telégrafo, 2016).

Según Kaspersky Laboratorio, mediante un análisis de amenazas en tiempo real, en junio del 2017 detecto que Ecuador ocupó en América del Sur el primer lugar con el 2,8 % y el quinto lugar a nivel mundial en cuanto a ciberataques a sus redes. El 49,05 % de estos fueron ocasionados mediante fuerza bruta a sus servidores de RDP ataques ocasionados mediante IPS y puertos TCP predeterminados en la infraestructura de sus servidores, ataque que permite y da la facilidad a los ciberdelincuentes o hackers el control total de todos los recursos almacenados (Alvarado,2020).

En el Ecuador las empresas u organizaciones, en su mayor parte no cuenta con una certificación de normas y políticas estandarizadas, que permitan el uso y su implementación en la infraestructura de su red en base a seguridad informática, motivo por el cual sufren ataques e infecciones de malware, ransomware ente otros afectando la integridad de sus recursos tecnológicos.

El Hospital General Alfredo Noboa Montenegro, no cuenta con una guía o modelo de manejo ante incidentes de seguridad informática, en sus activos informáticos e infraestructura de red, motivo por el cual con el pasar de los años empiezan a presentar fallos físicos y lógicos dando lugar a la presencia de vulnerabilidades y amenazas.

La investigación se realizó en el departamento de TI del "Hospital General Alfredo Noboa Montenegro", trabajo que fue factible realizarlo ya que se contó las facilidades brindadas por el Gerente y el apoyo del personal del área de tecnologías, se realizó un análisis de carencias y problemas que presenta el recurso informático y tecnológico con el que cuenta la entidad gubernamental y las mejoras que se va tener mediante el procedimiento de gestión de seguridad informática establecido. Desde el punto de vista económico el proyecto fue viable ya que no genero algún tipo de inversión o recursos extras a la institución.

Mediante el estudio se quiere contribuir en las actividades diarias en el área de TI por parte del personal de la institución "HGANM", con el análisis de normas, políticas y métodos de tratamiento de riesgos de incidentes informáticos, que

permita establecer un modelo de buenas prácticas para su infraestructura informática.

El principal beneficiario de esta investigación en la gestión de la seguridad informática será el "HGANM", y sus respectivos departamentos integrando políticas y normas estandarizadas de seguridad informática, garantizando la confiabilidad, integridad y disponibilidad de sus activos.

Los resultados de la investigación están estrictamente protegidos y publicados en base a la técnica aplicada para la gestión de la seguridad informática.

1.3. Objetivos

1.3.1. General.

Realizar un procedimiento para la gestión de la seguridad informática perimetral en la infraestructura de una organización.

1.3.2. Específicos.

- Analizar normativas, estándares y modelos existentes de seguridad informática.
- Aplicar un modelo de gestión de seguridad informática para la infraestructura de una Organización.
- Validar el modelo de gestión de seguridad informática en la Institución "Hospital General Alfredo Noboa Montenegro".

CAPITULO II

MARCO TEORICO

2.1. ANTECEDENTES INVESTIGATIVOS

En el trabajo de investigación Lozada (2019), realizó un "ESTUDIO DE LA SEGURIDAD INFORMÁTICA EN EL SECTOR DE TELEFONÍA MÓVIL EN ECUADOR PARA LA CREACIÓN DE MEDIDAS DE PROTECCIÓN DE LA INFORMACIÓN", trabajo que se centra en un análisis de las vulnerabilidades y amenazas que pueden causar daño, perdidas y acceso no autorizado a la información confidencial que manejan las operadoras móviles en el Ecuador, mediante que normas de telecomunicaciones prestan sus servicios de comunicación y que políticas de seguridad informática garantizan la protección de los datos de sus usuarios finales, en donde se destaca lo siguiente:

> Proponer el uso de la norma ISO 27001:2013, para el tratamiento de la información que manejan las empresas telefónicas en el Ecuador, en base a sus políticas y buenas prácticas que esta ofrece, además la implementación de un SERVICE DESK que permita gestionar de una forma eficiente los incidentes y garantizar la integridad de los datos e información de sus usuarios.

En la investigación de BOHEN et al. (2023), "SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS UNIVERSITARIOS", trabajo de investigación que expone sobre los riesgos y retos a los cuales están propensos los sistemas informáticos de las universidades ante los ataques informáticos causados por ciberdelincuentes y hackers, concluyendo con un aspecto importante que sobresale:

> Establecer un modelo de gestión de seguridad informática, basado en normas, políticas y estándares de acorde a la infraestructura de la universidad, que permita realizar auditorías periódicas y análisis de vulnerabilidades a su sistema informático

En la investigación de Almeida (2022), sobre "DISEÑO DE UN PLAN DE SEGURIDAD INFORMATICA PARA MIPYMES" trabajo que expone los riesgos a los que las MiPymes nacionales están expuestos al no contar con un plan de seguridad informática, que permita garantizar la información de sus activos, difusión de sus catálogos de servicios, teniendo como consecuencia el robo de información y acceso no autorizado a sus datos por ciberdelincuentes, llegando a una solución importante para el campo empresarial como es lo siguiente:

> Proponer a las Mi Pyme a invertir en la implementación de un plan de seguridad para la protección de la información el cual se base en la norma técnica de estandarización de políticas (NTC- ISO/IEC 27001:2013), con la finalidad de poder disminuir los riesgos mediante el aseguramiento, confidencialidad e integridad de los datos se sus sistemas informáticos.

Según Pazmiño (2019), mediante su estudio "DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA COOPERATIVA DE AHORRO Y CRÉDITO CHIBULEO LTDA., BASADO EN LA NORMA ISO/IEC 27002:2013", donde trata sobre la problemática que presenta el país, en la falta de políticas de seguridad de la información que permita reaccionar a la organización ante ataques informáticos que pueden afectar su estructura institucional, donde un aspecto importante fue:

> Interpretar la situación actual de la infraestructura de TI de la organización mediante la matriz de riesgos de Deloitte (2015), donde en base a un diagnóstico basado en la norma internacional ISO 27002:2013, permita identificar los controles aplicables a la infraestructura y proponer un diseño de la política de seguridad de información para el área de Tecnología de Información, con el fin de mitigar eventos de alto riego

Acosta (2022), plantea una "PROPUESTA BASADA EN LA SEGURIDAD LÓGICA PERIMETRAL EN LAS PYMES, COMO ESTRATEGIA PARA LA PROTECCIÓN CONTRA CIBERATAQUES" donde trata sobre los riesgos a los que están expuestos las empresas al no contar un sistema de seguridad informática y la importancia que

este conlleva en base a la seguridad protección de los datos, protección de activos informáticos y confidencialidad de la información, estudio que resalta:

> La elaboración de un Sistema De Gestión De Seguridad De La Información (SGSI), basado normas estandarizadas como la ISO/IEC 27001 que sirve como guía de actividades para el desarrollo del SGSI, la norma ISO/IEC 27002 que se encarga de los controles de seguridad (CIS) y marco de ciberseguridad (NIST), siendo necesarios para una adecuada gestión de riesgos de seguridad informática y protección ante ciberataques, plan que servirá como una guía de buenas prácticas de seguridad perimetral ante los ciberataques.

2.2. FUNDAMENTACIÓN CIENTIFICA

2.2.1. Seguridad Informática.

2.2.1.1. Definición.

La seguridad informática es un conjunto de herramientas y medidas que impiden la ejecución de actividades sin autorización, sobre la infraestructura de red de una organización, empresa e institución con la finalidad de prevenir posibles daños perjudiciales a los sistemas informáticos, así como evitar poner en riesgo la integridad, autenticidad y confidencialidad de su información.

2.2.1.2. Diferencia entre Seguridad Informática y Seguridad de la Información.

Partiendo de conceptos técnicos se define que, la Seguridad Informática trata o se centra específicamente en el tratamiento de amenazas y vulnerabilidades a la infraestructura tecnológica, es decir su principal función es proteger sus activos empleando soluciones técnicas. Mientras que la Seguridad de la Información se enfoca en la aplicación de técnicas, esquemas normativos, análisis de riesgos y utilización de buenas prácticas que garantizan la integridad de la información.

2.2.1.3. Pilares de la Seguridad Informática.

La seguridad informática (SI), se puede definir como los controles que se implementan con la finalidad de asegurar y proteger la información de personas no autorizadas, tomando en cuenta los siguientes pilares de la seguridad informática:

- **Confidencialidad. -** Es un elemento de la seguridad informática, donde la información es accesible solo para el personal autorizado.
  Según Tejada (2021), también se le conoce como NEED-TO-KNOW, término que hace referencia que a la información solo debe ponerse en conocimiento de las personas, entidades o sistemas autorizados para su acceso.

- **Integridad. -** Es el principal pilar de la seguridad, debido a que se encarga de salvaguardar y respaldar la información, con el objetivo que no sea borrada, copiada o alterada por terceros sin tener los permisos autorizados para modificar los datos cuando sea necesario.

- **Disponibilidad. -** Se refiere a que los datos e información deben estar disponibles para los usuarios al momento que se necesite.

Figura 1.

Pilares de la Seguridad Informática.

Nota: La figura detalla los pilares fundamentales de seguridad informática. Elaborado por (D. Peña, 2023).

2.2.1.4.Amenazas de la seguridad de la información.

Amenaza se define como todo lo que pueda generar daños en base a un incidente no deseado, este puede ser de tipo lógico o físico llegando a provocar en los activos de una organización la perdida de información, fallos en los equipos tecnológicos, etc.

Entre algunos tipos de amenazas se detallan las siguientes:

Virus informáticos o código malicioso: son programas o aplicaciones informáticas que acceden al sistema de una organización con la intención de causar daños sus sistemas, de forma intencional y sin el consentimiento.

Según Romero et al. (2018) los virus informáticos causan daños en el sistema operativo, eliminan archivos y perdida de información entre los diferentes tipos de virus existen los siguientes:

- Virus de sector de arranque (BOOT)
- Gusanos.
- Troyanos.
- Virus de archivos ejecutables.
- Malware.
- Virus de lenguajes de Script.
- Keyloggers, entre otros.

Ingeniería social: Se basa exclusivamente en la manipulación a la naturaleza humana, con la finalidad de obtener información confidencial de seguridad personal o empresarial que no debe ser compartida.

Uso no autorizado: consiste en el acceso indebido a un sistema de información, con fines de carácter intelectual o personal.

Denegación de Servicios (DoS): sirve para inhabilitar el correcto funcionamiento de un sistema, con la finalidad de bloquear y consumir los recursos que ofrece los servicios.

Robo de identidad: consiste cuando se obtiene información ajena, sin autorización con la finalidad de cometer actividades fraudulentas**.**

2.2.1.5. Mecanismos preventivos en seguridad informática.

Las organizaciones en su mayoría ven a los mantenimientos preventivos en la seguridad informática, como un proceso poco necesario y un costo adicional de inversión que con el tiempo no es recuperable, siendo uno de los aspectos para no considerar su debida importancia dentro de la estructura de las instituciones.

Romero et al. (2018), define que los mecanismos preventivos cumplen con la función de disminuir los ataques informáticos en la infraestructura de la empresa, realizando revisiones periódicas en hardware y software con la finalidad de aplicas cambio o mejoras si son necesarios.

Entre algunos procesos importantes que se pueden aplicar para los mecanismos preventivos son:

- **Respaldo de información. -** formatos de archivos se almacena (Archivos de texto, Base de Datos, Imágenes, Videos y Otros)
- **Control de medios. –** contar con accesos a respaldos de información es muy importante.
- **Actualización de sistemas.** – Realizar actualizaciones periódicas a los sistemas operativos, correcciones de errores y parches de seguridad, etc.
- **Contraseñas.** - Debe ser robusta, con una combinación de símbolos, letras y números, no se debe usar la misma contraseña para múltiples cuentas.
- **Accesos remotos. –** con el impacto a nivel mundial debido a la pandemia (Covid-19), las organizaciones se vieron en la obligación de emplear la modalidad de (Tele-Trabajo) para cumplir con sus actividades, garantizando una conexión segura para proteger su información.
- **Antivirus y Firewall. –** Los equipos tecnológicos deben conta con un antivirus actualizado para su protección al igual que un filtro de control de seguridad.

2.2.1.6. Mecanismos correctivos en seguridad informática.

Los mecanismos correctivos suelen aplicarse como consecuencia de no cumplir con un proceso adecuado de la ejecución de los mecanismos preventivos, es decir su

principal función es corregir las consecuencias; donde las empresas deben invertir en la adquisición de soluciones que permitan resolver los problemas.

Dentro de los mecanismos de corrección se tienen diferentes pasos de ejecución para enfrentar este problema, son los siguientes:

- **Catalogación y asignación de problemas. -** Se realiza un catálogo de problemas con la finalidad de detectar a que situación nos enfrentamos como ataques informáticos de ransomware, phishing, spam, robo de identidad entre otras cosas recurrentes en seguridad informática, con la finalidad de buscar una solución.
- **Análisis del problema. -** Tiene la principal tarea de analizar el problema presentado su afectación e impacto, el cual es analizada por los expertos en la materia y no por terceros involucrados en el problema.
- **Análisis de la solución. -** Encontrado el problema se debe plantear la propuesta de la solución, donde se analice los errores ocasionados de forma directa por lo usuario o por terceros, luego de validar la propuesta establecer los mecanismos de seguridad a implementar.
- **La documentación. -** Es de vital importancia respaldar un reporte de lo que paso y la propuesta de solución a implementar con la finalidad de evidenciar las debilidades y cambios que se realizó en un tiempo limitado, siendo necesario partir de una propuesta con la finalidad de fortalecer mejoras en seguridad.

2.2.1.7. Mecanismos de detección en seguridad informática.

Los mecanismos de detección requieren de un alto de grado de conocimientos, dependiendo de la materia y área relacionada como la seguridad, gestión de bases de datos y aplicaciones en el sistema que se está trabajando.

En el trabajo de investigación Romero et al. (2018), define que la detección de intrusos es una parte importante en este tipo de mecanismos, con la finalidad de seguir un proceso de identificación y respuesta ante procesos indebidos en el sistema e infraestructura de la red.

2.3. Vulnerabilidades

Son debilidades o fallos en los sistemas de información, comprometiendo su integridad y confidencialidad de los datos.

Romero et al. (2018), en su investigación define a vulnerabilidad como un fallo en el sistema, que al ser explotada por un atacante genera un riesgo para la organización o para el mismo sistema.

Vulnerabilidades Físicas. - Las vulnerabilidades físicas, son las que principalmente están relacionadas con la afectación de la manera física de la infraestructura de la organización, como la ubicación inadecuada de los equipos tecnológicos, mal diseño de distribución de cables de energía y red de datos, falta de supervisión de los controles de acceso a la información de la empresa, así como causan ambientales incendios, inundaciones, contaminación y cortocircuitos.

Vulnerabilidades lógicas. – Son vulnerabilidades que afectan directamente la infraestructura tecnológica y la operación de los mismos.

- **Configuración. –** Son vulnerabilidades exclusivas del sistema operativo que utilizan los equipos tecnológicos de la empresa, fallas de configuración, defectos de fabrica del sistema, versiones desactualizadas de aplicaciones, fallas de configuración de firewalls y servidor.

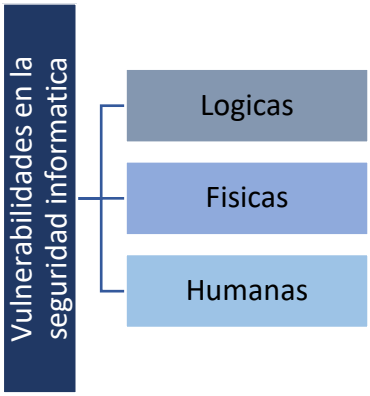
- **Actualización. –** Estas se presentan cuando la empresa no realiza supervisiones periódicas de las versiones actualizadas de sus sistemas operativos, programas sin licencia, conservaciones de equipos tecnológicos deficientes, falta de aplicación de antivirus, motivo por el cual la infraestructura suelen presentar vulnerabilidades o fallas.
- **Desarrollo. -** Son vulnerabilidades que se encuentran en el desarrollo y configuración de base de datos mediante código en SQL, Cross Site Scripting, su variación depende del tipo de aplicación y la validación de los datos.

Vulnerabilidades Humanas. - Son las que se presentan con mayor continuidad en la infraestructura de la organización, por falta de concientización y capacitación al

personal, negligencia o curiosidad de los usuarios, falta de determinación de responsabilidades, desarrollo de políticas de buenas prácticas, falta de seguimiento de políticas y procedimientos de seguridad, falta de cumplimiento de plan de contingencia.

Figura 2

Vulnerabilidades en la Seguridad Informática.



Nota. La figura muestra la clasificación de las vulnerabilidades de la seguridad informática. Elaborado por (D. Peña,2023).

2.4. Importancia y beneficios de la seguridad en las organizaciones.

Las empresas y organizaciones buscan proteger su sistema de información, con el objetivo de ser un competidor en el mercado empresarial en el ámbito de seguridad, protegiendo su infraestructura de ataques ocasionados por terceros ante cualquier vulnerabilidad que le facilite realizar ataques informáticos.

Según la ISO/IEC (2016), la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos.

En cuanto a los beneficios que la seguridad de la información ofrece se destaca los siguientes:

Reducción de costes: Incide en el aspecto económico de todo tipo de organización en el campo de la seguridad, donde la gestión del sistema de información en un corto plazo evitara sufrir pérdidas económicas para la organización.

Protección del negocio: un sistema de seguridad busca mediante planes de contingencia evitar interrupciones en las actividades o procesos de la organización, manteniendo la disponibilidad de sus activos y garantizando la continuidad del negocio.

Mantener y mejorar la imagen corporativa: Se ve reflejada directamente en la imagen de la organización ya que esta se percibe como empresa responsable, comprometida con la mejora de sus procesos, productos.

2.5. Sistema de Gestión de la Seguridad de la Información (SGSI).

2.5.1. Definición de un SGSI.

SGSI (Sistema de Gestión de la Seguridad de la Información), es una herramienta la cual mediante procesos busca velar por la seguridad de la información.

Un SGSI es un conjunto completo de controles de seguridad con la finalidad de implementar, operar, monitorear, revisar y mejorar la seguridad de la información de una organización.

Rodríguez (2016), define a un SGSI como un conjunto de procesos que permitan gestionar de una manera eficiente la accesibilidad de la información y garantizar la confidencialidad, integridad y disponibilidad de sus activos al igual que un manejo adecuado de los riesgos a los que esta expuestos la información.

En su estudio de investigación Lucano (2019), define al Sistema de Gestión de Seguridad de la Información como el conjunto de políticas, procesos, guías y estructuras que se relacionen con la finalidad de proteger su activo más importante, la información.

Uno de los objetivos principales de la materia de seguridad de la información es reducir el riesgo de la información en la organización. Este término, acorde con la norma ISO/IEC 27000, está asociado a preservar elementos relacionados a la confidencialidad de información (Valencia, 2017).

2.5.2. Alcance de un SGSI.

En un SGSI el alcance depende principalmente de la ubicación de los activos de información importantes, con el objetivo de analizar una parte o toda la infraestructura de la organización, entre los alcances y partes que no hayan sido consideradas tenemos:

- Políticas de seguridad: determina el compromiso de las direcciones de la organización.
- Métodos de control que soportan al SGSI: normalizan su propio funcionamiento.
- Enfoque de Evaluación de Riesgos: procedimiento a plantear de criterios de aceptación de riesgos y de niveles aceptables.
- Reporte y Evaluaciones de Riesgos: se analizan los resultados después de aplicar lo mencionado a los activos de la organización.
- Proponer un Tratamiento de Riesgo: determina las acciones de los tratamientos del riesgo de seguridad de la información en función de lo obtenido como conclusiones.
- Procedimientos documentados: se enfoca en mantener seguridad en la planificación, operación y control de los procesos de seguridad.
- Registros: facilita la evidencia de la eficacia de los SGSI.
- Declaración de Aplicabilidad: contiene los objetivos de control y los controles contemplados por el SGSI.

2.5.3. Beneficios de un SGSI.

Los principales beneficios que tiene una empresa u organización, con la implementación de un Sistema de Gestión de Seguridad de la Información son:

- Minimizar el riego de perdida de información en las organizaciones.
- Manejo eficiente de gestión de riesgos con la finalidad de identificar amenazas y vulnerabilidades que se presenten en las actividades de la organización
- Permite administrar la seguridad de la información y establecer mejoras competitivas, fortaleciendo un grado de confianza en la organización.

- Establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.
- Contar con SGSI permite mejorar la imagen de la empresa, obteniendo un crecimiento comercial para la organización, así como, obtener méritos con los clientes
- Prevenir y detectar de manera eficiente y anticipada incidentes de seguridad de la información.
- Promueve reducción de costos y una mejor operación de los procesos, debido a la reducción de incidentes de seguridad de la información
- Contar con procedimientos y procesos que permitan reaccionar al generarse un problema, con la finalidad de garantizar la continuidad y disponibilidad de las operaciones de una organización.

2.5.4. Metodologías de Análisis y Gestión de Riesgos.

El análisis de riesgos permite determinar los factores de riesgo y afectación de un proyecto una vez identificado y clasificados los riesgos, además estudiar la posibilidad y consecuencias de cada factor de riesgo y su nivel de impacto

En el estudio de investigación Rodríguez (2016), que para la implementación de un SGSI es primordial realizar una correcta gestión de riesgos en base a las vulnerabilidades presentes en los activos de información y las principales amenazas que pueden explotar estas vulnerabilidades, con la finalidad en establecer medidas preventivas y correctivas que garanticen la seguridad de la información y sus activos principales.

En el proyecto de investigación Guacanés et al (2022), indica que los métodos de análisis de riesgos sirven para evaluar los riesgos de un trabajo o proyecto, con la finalidad de implementar medidas de prevención y reducir su impacto de afectación.

Existen varias metodologías utilizadas para la gestión de riesgos, que parten de un procedimiento similar, con la identificación de activos de información, identificación de las amenazas o riesgos y las vulnerabilidades.

2.5.4.1. MAGERIT.

MAGERIT se define como un proceso de gestión de riesgo, que permite a las instituciones públicas o privadas tomar decisiones en base a los riesgos a los que están expuestos sus activos con el uso de las tecnologías de la información (Bonilla,2018).

El método de MAGERIT fue desarrollado por el Ministerio de Administración Publicas, su principal función es seguir un proceso que permite evaluar el estado de los riesgos, gestionar su mitigación y llevar un control practico mediante un análisis y una gestión efectiva (Pardo,2015).

El análisis de los activos mediante el método de MAGERIT se basa específicamente en 3 documentos:

- Libro I: Método
- Libro II: Catálogo de Elementos
- Libro III: Guía de Técnicas,

La metodología tiene como finalidad los siguientes objetivos.

Indirectos.

- Preparar a una institución para que responda de una forma efectiva y ordenada ante procesos de evaluación, auditoria y acreditación.

Directos.

- Crear un ambiente de concientización y responsabilidad a los encargados de gestionar los activos de información, ante riesgos existentes.
- Aplicación de proceso sistemático que permite el análisis de riesgos con el uso de tecnologías de información y comunicaciones.
- Permite descubrir e implementar procesos de mejora que permitan tratar de forma oportuna los riesgos que se pueden presentar en los activos de una institución.

2.5.4.2. OCTAVE

El método de Octave (Operacional Critical, Threat, Asset and Vulnerability Evaluación), desarrollado por el Departamento de Defensa de la Universidad Carnegie Mellon de los EEUU.

Es una metodología que propone mediante una base de criterios y guías específicas de administración, evaluar los riesgos que están expuestos los activos y proponer un plan de mitigación para controlarlos (Mendoza et al, 2020).

Octave es una de las metodologías de análisis de riesgos más empleadas en empresas grandes y pequeñas, debido a que permite identificar riesgos en los activos existentes de una institución y emplear planes de mitigación en base a sus criterios definidos (Bravo,2018).

En la metodología Octave para su análisis de riesgos: propone diversos procesos como la evaluación de activos de seguridad de información, asignar un valor a cada activo y finalmente analiza como esta estructura la infraestructura para identificar los activos importantes para la organización (Guano & Jaramillo,2020).

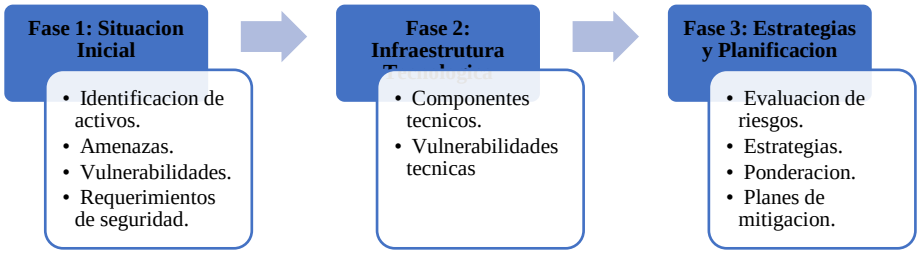
La metodología de Octave cuenta con 2 versiones.

- Octave-S (metodología para organizaciones pequeñas).
- Octave Allegro (metodología para organizaciones con estructuras multinivel).

OCTAVE, se basa en 3 fases específicas que permite y facilita a la organización tener una idea clara de las necesidades en el campo de seguridad de la información.

Figura 3

Planificación metodología de OCTAVE.



Nota: La figura detalla las fases de estructuración de la metodología de OCTAVE. Elaborado por (D. Peña, 2023).

Fase 1: se realiza una identificación de activos con los que cuenta la organización, los cuales se los clasificara para poder evaluar las amenazas y vulnerabilidades que pueden presentar.

Fase 2: analizar la composición de la infraestructura de la organización para determinar las principales amenazas críticas que pueden afectar la seguridad de la información.

Fase 3: definir el personal apto y capacitado para realizar el análisis de los riesgos, que permita evaluar las amenazas, así como el desarrollo de un plan de mitigación que permita disminuir o controlar los niveles de riesgos.

2.5.4.3. NIST 800-30.

NIST SP 800 – 30 (National Institute of Standards and Technology), es una guía de gestión de riesgos compuesta por un conjunto de actividades y recomendaciones que tienen como finalidad ayudar a las organizaciones a gestionar de una mejor manera los riesgos, mitigar, analizar y evaluar el riesgo (National Institute of Standards and Technology, 2012).

NIST 800-30 es el método de riesgos es el más utilizado en empresas grandes debido a su robusta estructura de seguridad CIA, lo que permite en el desarrollo de proyectos de TI tener un análisis de riesgos eficiente y satisfactorio al momento de valorar las amenazas y sus impactos en relación a los activos de la organización (Guano & Jaramillo, 2020).

La metodología NIST SP 800-30, tiene como objetivos.

- Aseguramiento de sus sistemas de información.
- Gestión de Riesgos.
- Optimizar su administración y resultados de análisis de riesgos.

Pasos para cumplir con su proceso de análisis de riesgos:

Evaluación del Riesgo: se emplea para determinar el grado de impacto ante una posible amenaza y su riesgo dentro de un sistema de información. Para la evaluación de riesgos se debe seguir los siguientes pasos:

- Caracterización del sistema.
- Identificación de amenazas
- Identificación de vulnerabilidades.
- Análisis de control.
- Cálculo de Probabilidad
- Análisis de Impacto.
- Determinación del riesgo.
- Recomendaciones de control.
- Documentación de resultados.

Mitigación del riesgo: consiste en evaluar e implementar controles apropiados para reducir los riesgos en base a una evaluación del riesgo, donde se cuenta con las siguientes alternativas:

- Asumir el riesgo: aceptar el riesgo potencial o crear e implementar controles con la finalidad de reducir el riesgo a un nivel aceptable.
- Evitar el riesgo: eliminar las causas del riesgo.
- Reducir el riesgo: emplear controles que permitan minimizar los riesgos con un impacto negativo de la amenaza que no permita explotar su vulnerabilidad.
- Transferir el riesgo: utilizar o emplear otras alternativas.

Análisis y Evaluación: debido a que los riesgos pueden cambiar con el paso del tiempo debido a cambios de hardware y software en la infraestructura de la organización, existiendo nuevos riesgos en los activos, por lo que para el inicio de su evaluación es importante partir de las siguientes medidas:

- Plan actual.
- Recurrir un plan de contingencia.
- Re-plan.
- Cerrar el riesgo.

2.6. Normas ISO.

Figura 4

Organización Internacional de Estandarización (ISO).

Nota: La figura muestra las características y funciones de la Norma ISO. Tomado de (Norma ISO, 2013)

La Organización Internacional de Estandarización (ISO), es un organismo no gubernamental creada el 23 de febrero de 1947 con el objetivo de promover la implementación de normas a nivel internacional para brindar herramientas que faciliten las transacciones a nivel internacional tanto de objetos, bienes y servicios como de desarrollos científicos, actividades intelectuales, tecnológicas y económicas. La organización está constituida por 180 Comités Técnicos y las actividades técnicas se encuentran descentralizada en unos 2700 Comités, subcomité y grupo de trabajo que proponen las nuevas normas, participan en su desarrollo y ofrecen el apoyo, conjuntamente con la Secretaría General de la ISO.

Ducuara (2017), ISO considera como una organización a nivel mundial que se concentra en normas de estandarización y buenas prácticas, que permitan establecer una mejora continua a la infraestructura de distintas instituciones. Su objetivo es la promoción para que se lleven a cabo estandarizaciones internacionales.

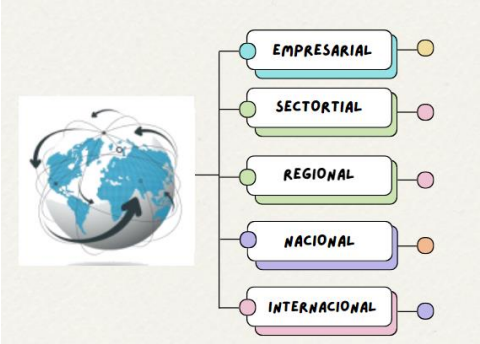
ISO son normas internacionales que son desarrolladas a partir de un consenso de grupos de las partes interesadas, que buscan mediante la contribución de varios expertos identificar y elaborar normas necesarias para el comercio, los gobiernos y la sociedad en general, para su implementación y validación de resultados.

Gómez et al (2008), las normas ISO facilitan el comercio Internacional a medida que dicha actividad adopta formas más complejas de realización, la importancia de las normas se acrecienta; hoy en día no podríamos pensar en un mercado común sin Normalizar los productos a intercambiar.

2.6.1. Alcance de las normas ISO.

Figura 5

Alcance Norma ISO.



Nota. La figura muestra el alcance de la Norma ISO en el mundo global.

- **Empresarial. –** Son normas editadas e implantadas en una compañía gubernamental o de iniciativa privada, originadas y reconocidas por el cuerpo directivo, donde se establece características o directrices, con el objetivo de tener eficiencia en el control, actividades y procesos.

- **Sectorial. -** Son normas editadas y reconocidas por un conjunto de empresas relacionado en algún campo industrial determinado, con la finalidad de evitar competencias desleales entre los fabricantes.

- **Nacional. –** Son normas que a través de una organización nacional privada o gubernamental, son desarrolladas en base a intereses que pueden afectar a un país, en la mayoría estas normas son validadas y homologadas por los países desarrollados, siendo adoptadas por los demás países en subdesarrollo.

- **Regional. –** Son normas editadas e implantadas por un grupo de países de la misma región geográfica, con el fin facilitar un mejor intercambio tanto económico como de transferencia tecnológica entre los mismos.

- **Internacional. -** Es el nivel de Normalización que presenta el esquema de aplicación más amplia y cuyas normas son el resultado, en muchas ocasiones de arduas sesiones para conciliar los intereses de todos los países que

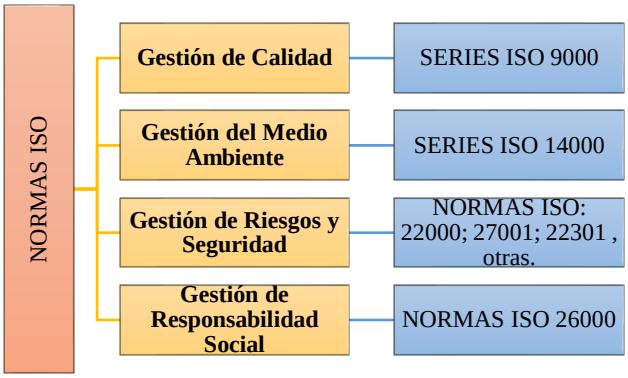
intervienen en el proceso, actualmente el organismo que agrupa la gran mayoría de los países del orbe (82) es la ISO (International Standard Organización).

2.6.2. Familia de Normas ISO

Las normas ISO se van actualizando periódicamente motivo por el cual aparecen nuevas y existen una gran cantidad de normas, clasificadas o agrupadas por familias o series con el objetivo de contar con una nomenclatura específica para su aplicación eficiente según al campo que corresponda.

Figura 6

Familia Normas ISO.



Nota. La figura muestra la clasificación de la Norma ISO, e acuerdo a cada área de trabajo. Elaborado por (D. Peña, 2023).

2.6.3. ISO 27001

La revisión de esta norma fue en el 2013, año en el que pasó a denominarse ISO/IEC 27001:2013. Su primera revisión, cabe recordar, fue ocho años antes. Asimismo, la ISO 27001 puede ser implementada en todo tipo de entidad, sea privada o pública, pequeña o grande, con o sin fines de lucro.

La ISO 27001 es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI). El objetivo de esta norma es proporcionar un marco o modelo robusto para establecer, implementar, operar, revisar, mejorar y proteger la

información que se puede adaptar a organizaciones de todo tipo y tamaño (ISO 27001, 2013).

La norma ISO 27001 establece control de política de seguridad, gestión de activos, seguridad de recursos humanos, comunicaciones y operaciones, control de acceso, gestión de incidentes de seguridad, continuidad de negocio y mejoras de seguridad de la información (ISO 27001,2013).

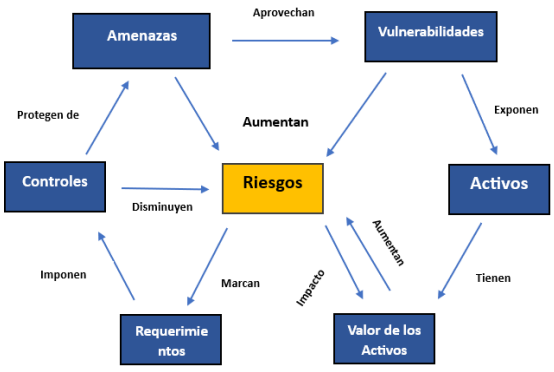
2.6.3.1. Principios y Terminología.

Los riesgos en la seguridad de la información generalmente surgen debido a la presencia de amenazas para los activos que procesan, almacenan, mantienen, protegen o controlan el acceso a la información, lo que da lugar a incidentes (ISO 27001,2013).

- Activos. – Suelen ser personas, equipos, sistemas o infraestructura.
- Información. – Conjunto de datos que una organización desea proteger, como los datos de empleados, clientes, financieros, plan de diseño, etc.
- Incidentes. – Son eventos no deseados que resultan en una pérdida de confidencialidad (violación de datos), integridad (corrupción de datos) o disponibilidad (fallo del sistema).
- Amenazas. – son las que causan incidentes y pueden ser maliciosas (como un robo), accidentales (un error tipográfico) o desastres ambientales (como una inundación).

Figura 7

Uso de SGSI.



Nota. La figura muestra el proceso de tratamiento de riesgos en un SGSI.

2.6.3.2. Ciclo PHVA.

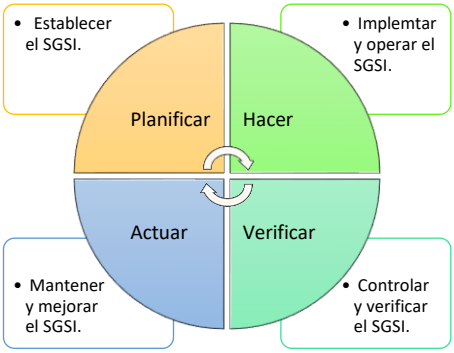
La ISO 27001 se basa en el ciclo PHVA, también conocido como ciclo de Deming que se puede aplicar tanto a un sistema de gestión en general o aun elemento individual con la finalidad de propones un enfoque de mejora continua.

La estructura del ciclo de Deming PHVA se basa o consta de 4 etapas que son:

- Planificar. – se considera la fase inicial de un SGSI donde se crean estrategias, políticas, objetivos, recursos, identificación de riesgos y oportunidades para la mejora de la seguridad de la información de una organización.
- Hacer. – Es la fase donde se va implantar y gestionar el SGSI tomando en cuenta controles, procesos y procedimientos considerados en la fase inicial, en base a un entorno de pruebas se evalúa y valida los resultados para la implementación en un entorno real.
- Verificar. – Se encarga de monitoreo del SGSI con el objetivo de controlar y medir los procesos para establecer el rendimiento de la política, objetivos, requisitos y actividades planificadas e informar de los resultados.
- Actuar. – La fase final se encarga del mantenimiento y acciones para mejorar el rendimiento del SGSI adoptando medidas preventivas o correctivas para su buen funcionamiento, en caso de haber ocurrido algún problema el ciclo se debería repetir de nuevo.

Figura 8

Ciclo PHVA.



Nota. La figura muestra las etapas que cumple el ciclo de Deming. Elaborado por (D. Peña, 2023).

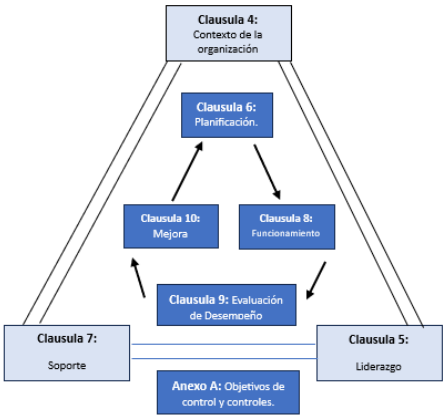
2.6.3.3. Requisitos.

La norma ISO/IEC 27001 es la más relevante y fundamental dentro de la familia ISO/IEC 27000, está diseñada para ser aplicable a cualquier tipo de organización, independientemente del tamaño, la complejidad, el sector industrial o el propósito ya que establece los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones (ISO 27001, 2013).

En el Anexo A de la norma ISO/IEC 27001 se encuentran los objetivos de control y los controles que se basan en la gestión de riesgos y promueven la mejora continua de los procesos (ISO 27001, 2013).

Figura 9

Estructura de la norma ISO 27001.



Nota. La figura muestra las cláusulas estructuradas en la Norma ISO 27001. Tomado de (ISO 27001, 2013).

2.6.3.4.Amenazas y Vulnerabilidades en ISO 27001.

Las amenazas y vulnerabilidades son abordadas en el capítulo 8 de la norma ISO 27001, son conceptos importantes ya que la existencia de un riesgo depende de la coexistencia de una amenaza y una vulnerabilidad.

Según la norma ISO/IEC 27001 las vulnerabilidades se refieren a fallos o debilidades presentes en un activo, por otro lado, las amenazas son situaciones que pueden desencadenar o aprovechar una vulnerabilidad para comprometer algún aspecto del activo.

Tabla 1

Amenazas y Vulnerabilidades en ISO 27001.

VULNERABILIDADES	AMENAZAS
• Falta de redundancia. • Fallas de control de acceso físico. • Faltas de políticas de acceso remoto. • Software no licenciado. • Conexiones desprotegidas. • Desprotección en equipos móviles. • Mantenimiento deficiente. • Falta de control datos E/S. • Respaldo inapropiado. • Falta de políticas para el uso de criptografía. • Eliminación de medios de almacenamiento. • No existencia de sistemas de autenticación. • Mala gestión de la capacidad del sistema. • Deficiente implementación de auditoría interna. • Falta de especificaciones de desarrollo de software. • Inadecuada gestión de red.	• Acceso a la red no autorizado. • Comprometer información confidencial. • Daños ocasionados por terceros. • Fuga de información. • Perdida de energía eléctrica. • Divulgación de contraseñas. • Código Malicioso. • Ataques bomba. • Revelación de información. • Instalación no autorizada de software. • Infracción legal. • Uso indebido de sistemas de información. • Errores de mantenimiento. • Destrucción de registros. • Fallos de comunicación. • Mal funcionamiento de equipos.

Nota. La tabla muestra la clasificación de posibles amenazas y vulnerabilidades de seguridad informática.

2.6.4. MARCO LEGAL.

2.6.4.1. Ley Orgánica de Protección de Datos Personales de Ecuador

La Asamblea Nacional del Ecuador, en sesión virtual No. 707 del 10 de mayo de 2021, aprobó el proyecto de Ley Orgánica de Protección de Datos Personales de Ecuador (LOPDP), el cual tras los correspondientes debates y sancionado por el señor presidente de la Republica se publicó el 26 de mayo del 2021 (LOPDP, 2021).

La Ley de Protección de Datos Personales establece disposiciones que deben cumplir tanto las entidades del sector público como del sector privado, para lo cual cuentan con un período de adaptación de dos años con el objetivo de poder adecuar todos sus procesos a lo exigido por esta nueva normativa (LOPDP, 2021).

La LOPDP tiene como objetivo garantizar el ejercicio del derecho a la protección de datos personales, base de datos, con la finalidad de mejorar la relación de las empresas con sus clientes garantizando la integridad y confidencialidad de sus datos personales evitando su uso para otros fines (LOPDP, 2021).

2.6.4.2. Principios de la LOPDP.

En base a los principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la LOPDP cuenta con 13 principios:

- ✓ Juridicidad
- ✓ Lealtad
- ✓ Transparencia
- ✓ Finalidad
- ✓ Pertinencia y minimización de datos personales
- ✓ Proporcionalidad del tratamiento
- ✓ Confidencialidad
- ✓ Calidad y exactitud
- ✓ Conservación
- ✓ Seguridad de datos personales
- ✓ Responsabilidad proactiva y demostrada
- ✓ Aplicación favorable al titular
- ✓ Independencia del control.

2.6.4.3. Derechos de la LOPDP.

Los datos personales en base a su norma regulatoria especializada en ejercicio de la libertad de expresión, sectores regulatorios, gestión de riesgos, desastres naturales, seguridad nacional y defensa nacional; así como los datos que se deben proporcionar a autoridades administrativas o judiciales en base a solicitudes y ordenes amparadas en normativa vigente, los cuales estarán sujetas a principios y normas establecidos en la Ley y mediante el cumplimiento de estándares internacionales en la materia de derechos humanos cumpliendo con los criterios de legalidad, proporcionalidad y necesidad (LOPDP, 2021).

Figura 10

Derechos de LOPDP.

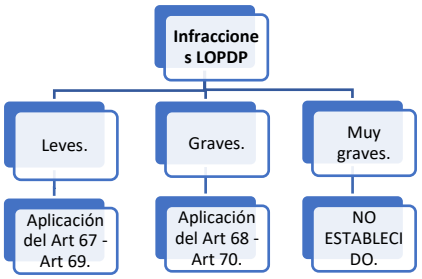
Nota. La figura define los criterios establecidos en los derechos de LOPDP.

2.6.4.4. Infracciones y Multas LOPDP.

Para el cumplimiento de los artículos establecidos en la LOPDP, se determinan las siguientes infracciones y multas, que se pueden cometer y aplicar durante el no cumplimiento de la ley (LOPDP, 2021).

Figura 11

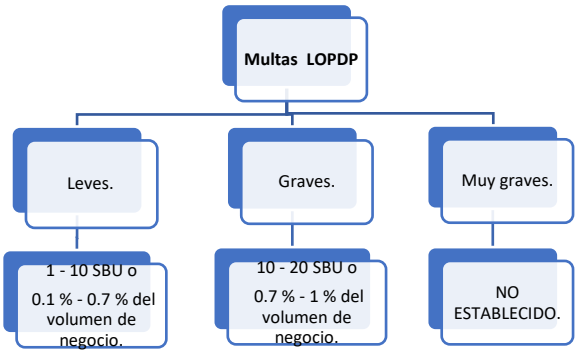
Infracciones establecidas en la LOPDP.



Nota. La figura detalla los tipos de infracciones definidos en LOPDP. Tomado de (LOPDP, 2021).

Figura 12

Multas según la Infracción en la LOPDP.



Nota. La figura detalla los tipos de infracciones definidos en LOPDP. Tomado de (LOPDP, 2021)

2.7. Herramientas de Pentesting.

El pentesting se define como un proceso de simulación de un hackeo o ataque la red de una organización de forma controlado, las pruebas son desarrollados por expertos o personas con conocimiento en seguridad de redes TI. Durante este análisis o monitoreo los escáneres de vulnerabilidades actúan para permitir al personal de seguridad es detectar y gestionar sus posibles vulnerabilidades en sus sistemas.

Los análisis o pruebas que se emplean para detectar posibles vulnerabilidades en la infraestructura de una organización como redes o dispositivos, son sumamente importantes para el conocer su nivel de seguridad (Cedeño,2022).

2.7.1. Tipos de Pentesting.

Test Intrusivo Externo: conocido como test de caja negra, se enfoca en verificar el nivel de seguridad de la red externa de la institución, el pentesting realiza un análisis sin conocer ninguna información sobre el sistema o aplicación por lo que se convierte en un atacante externo con el único objetivo de acceder a información confidencial comprometiendo la privacidad de la empresa.

El escaneo de vulnerabilidades externo se lo realiza fuera de la empresa, donde su principal objetivo es buscar un posible intruso o atacante que exponga la seguridad de la red, firewalls de seguridad o aplicaciones web (Hidalgo,2023).

Test Intrusivo Interno: conocido como test de caja blanca o caja gris, este método busca determinar qué nivel de seguridad interna cuneta la empresa, donde el pentesting cuenta con información confidencial, así como su arquitectura de red por lo que simula ser un atacante verificando la seguridad completa del sistema.

Su principal objetivo es encontrar vulnerabilidades en la red interna, permitiendo detectar sus puntos débiles o amenazas internas de seguridad por lo que es necesario aplicar parches que permitan proteger y cerrar brechas en el perímetro de la red (Hidalgo,2023).

2.7.2. Herramienta NESSUS.

Figura 13

Logotipo NESSUS.

Nota. La figura muestra una identificación de NESSUS en el mundo de seguridad.

Nessus es una herramienta de evaluación de vulnerabilidades utilizada a nivel mundial, aplicable en el campo de la industria para reducir los ataques y asegurar la infraestructura de las organizaciones. La interfaz de Nessus cuenta con características potentes que permiten la detección de activos de alta velocidad, auditoria de configuración, detección de malware y datos confidenciales con amplias funciones de gestión que son de fácil manejo para el ámbito de seguridad.

Nessus es compatible para varios sistemas operativos, tecnologías, firewalls, hipervisores de datos, servidores web, cuenta con una amplia biblioteca de vulnerabilidades y actualizaciones permanentes, cuenta con soporte de expertos de TENABLE, permite tener una velocidad y precisión al momento del escaneo en tiempo de real de las vulnerabilidades.

La aplicación de NESSUS dentro de las organizaciones da la posibilidad de proteger entornos físicos, virtuales y en la nube como puede ser de forma física y en la nube. Gracias a la plataforma de gestión de Tenable.io y a sus dos opciones de implementación con o sin agente facilita trabajar en entorno móviles, transitorios y difíciles de alcanzar.

Nessus es una herramienta sumamente utilizada en la ciberseguridad, debido a que permite identificar, evaluar y analizar las posibles debilidades y vulnerabilidades en

sistemas y dispositivos con el objetivo para la detección de posibles riesgos de seguridad (Hidalgo,2023).

Características de NESSUS.

Informes y Monitoreo.

- Generación flexible de informes de escaneo, con la finalidad de ordenar y comparar resultados de vulnerabilidades detectados en base de datos, XML, CSV y HTML.
- La recepción de notificaciones mediante correo electrónico, de los resultados de los escaneos, así como sus posibles remediaciones y correcciones

Capacidades de Escaneo.

Detección:

- Detección de alta velocidad de activos.

Escaneo:

- Escaneo de vulnerabilidades en Redes IPv4/IPv6/Hibridas.
- Detección de vulnerabilidades no acreditadas.
- Escaneo para refuerzo del sistema y parches faltantes.

Cobertura:

- Dispositivos de red como firewall, enrutadores e interruptores.
- Virtualización de máquinas VMware en Microsoft, Hyper-V, vCenter, etc.
- Compatibilidad en sistemas como Windows, Linux, Solaris, Cisco iOS, etc.
- En base de datos Oracle, SQL Server, PostgreSQL, etc.
- Cumplir con requerimientos y normas regulatorias y corporativas**.**

Amenazas:

- Auditoria de botnets.

- Detección de virus, contenido malicioso, malware en servidores y servicios web en la red.
- Auditorias de configuración en base a CERT, COBIT/ITIL, DISA STIG, FDCC, ISO, NIST, NSA, PCI.

Implementación y gestión.

- Flexibilidad al momento de implementar software, hardware ya sea desde un dispositivo virtual de manera local o en la nube de un proveedor de servicios.
- Admite escaneos remotos con o sin credenciales.
- Escaneos locales en línea o remotos.
- Configuración de políticas y plantillas de configuración.
- Evaluar los riesgos en base a cinco niveles de gravedad (crítico, alto, mediano, bajo, información).
- Filtrado por nivel de aprovechamiento y severidad.

Ventajas de NESSUS.

- Escaneo de alta precisión con bajo número de falsos positivos.
- Capacidades y características de escaneo integrales.
- Escalabilidad a cientos de miles de sistemas.
- Implementación y mantenimiento sencillos.
- Bajo costo de administración y operación.

2.7.3. Herramienta NMAP.

Figura 14

Logotipo NMAP.

Nota. La figura muestra la identificación de la herramienta NMAP.

NMAP es una herramienta de software abierto utilizado para analizar grandes redes, donde sus administradores utilizan esta herramienta para realizar tareas rutinarias, exploración red, auditoria de seguridad, actualización y monitoreo en tiempo real de los equipos o servicios activos en la infraestructura de una red.

NMAP utiliza él envió de paquetes IP que no han sufrido ningún tipo de modificación, permitiendo obtener la información de su servidor como su nombre y la versión que está utilizando, que sistema operativo tiene instalado y demás características que permite visualizar la aplicación mediante su escaneo de red (Cedeño, 2022).

La información importante que resalta la aplicación de NMAP en cualquier infraestructura de red es que permite visualizar los puertos y protocolos de servicio y su estado, como puede ser open (abierto), filtered (filtrado), closed (cerrado) o unfiltered (no filtrado).

Existen dos formas de utilizar NMAP, como puede ser:

- Mediante comando NMAP para consola.
- ZENMAP de manera grafica.

2.7.3.1. Funciones.

Entre las principales tenemos:

- Identificación de equipos conectados en la red.
- Identificar puertos y estado de los mismos.
- Conocer si está utilizando cortafuegos.
- Características de hardware de los equipos conectados.
- Detectar sistema operativo instalado y versión.

2.7.4. Herramienta Rapid7.

Figura 15

Logotipo Rapid7.

Nota. La figura muestra la identificación de la herramienta RAPID7.

Rapid7 es una empresa de seguridad cibernética que ofrece una amplia gama de sus productos y servicios, permite a las organizaciones analizar su infraestructura de TI con la finalidad de identificar vulnerabilidades, responder a amenazas, reducir riesgos, optimizar y fortalecer la seguridad de una organización.

Además, ofrece servicios de consultoría y capacitación en seguridad cibernética empleando tecnología avanzada en análisis de datos, conocimientos y herramientas necesarias para brindar soluciones en el área de seguridad, gestión de vulnerabilidades, automatización y análisis de seguridad para responder eficazmente ante las amenazas de seguridad para proteger sus activos (Hidalgo,2023).

Rapid7 es una herramienta monitoreo con una interfaz simple para su manejo, su principal objetivo la gestión de vulnerabilidades la cual, mediante un proceso activo, detecta exclusivamente todos los componentes de la red en tiempo real (Hidalgo,2023).

2.7.4.1.Características.

Cobertura de Activos.

Rapid7 da la posibilidad de realizar un análisis de las aplicaciones web y sus sistemas locales, aplicación que cuenta con mecanismos que permite detectar de manera completa los activos de una organización. Los contenedores en la nube funcionan mediante una API la cual requiere de un entorno cloud como lo es NEXPOSE.

Detección de Vulnerabilidades.

La detección de amenazas es el centro de todo software de gestión de vulnerabilidades, es recomendable realizar un escaneo pasivo y continúo potenciado por agentes de inteligencia de amenazas, políticas de auditoría y configuración de los distintos activos permita rastrear las debilidades de internet con el objetivo de salvaguardar su información y datos (Hidalgo,2023).

Automatización.

Rapid7 tiene la ventaja de reducir la operación de los departamentos de TI y Soporte, para lo cual es importante definir una herramienta con agentes inteligentes e integrados que permitan evaluar un host llevarlo al siguiente nivel de protección y atender sus vulnerabilidades prioritarias.

Gestión de Resultados.

La eficiencia de una herramienta de seguridad informática se la puede evaluar por la flexibilidad de implementación de software in-house y cloud, que permita realizar operación y actividades online, en base a protocolos de calidad y de seguridad. (Hidalgo,2023).

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo de investigación

Para el desarrollo del presente proyecto de investigación y en coordinación con el responsable del Área de Tecnologías de la Información del "Hospital General Alfredo Noboa Montenegro", la investigación a utilizar es:

3.1.1. Investigación Aplicada.

En el presente trabajo se empleó una investigación aplicada, porque se empleó los conocimientos estudiantiles, con el objetivo de investigar, analizar, encontrar y aplicar la metodología correcta e idónea.

3.1.2. Investigación Bibliográfica.

La investigación fue bibliográfica o documental con el objetivo de fortalecer conocimientos y recopilar información relevante de libros, revistas, artículos científicos, tesis, normas de seguridad y buenas prácticas, ley de protección de datos personales, sistema de gestión de seguridad de la información, etc.

3.1.3. Investigación de campo.

Se emplea una investigación de campo, en base a las instalaciones de la institución HGANM con el objetivo de recopilar información de los activos informáticos, sistemas operativos y procesos con los que trabaja cotidianamente el área de TI, para analizar los riesgos a los que se encuentra expuesto la red de datos de la institución.

3.1.4. Investigación Exploratoria.

El proyecto también empleó una modalidad de Investigación Exploratoria ya que se realizaron pruebas en los servidores para medir y garantizar la fiabilidad del resguardo de información, así como pruebas de monitoreo de amenazas y vulnerabilidades en los sistemas y activos del HGANM.

3.2.Población o muestra:

Para el desarrollo del trabajo de investigación, Procedimiento para la Gestión de la Seguridad Informática en el área de tecnologías del "Hospital General Alfredo Noboa Montenegro" no se requiere de muestra debido a que se trabajó con el 100% de personal encargado de administrar el área de Tecnologías de la Información.

3.3. Prueba de Hipótesis - pregunta científica – idea a defender

Considerando que el presente trabajo investigativo corresponde a un estudio de casos que tiene un alcance exploratorio no aplica el planteamiento de la hipótesis.

3.4. Recolección de información

Para el desarrollo de trabajo de investigación se utilizó como técnicas de recolección de información, como partida inicial se realizó una entrevista y encuesta dirigido al personal del área de Tecnologías como son: Analista de Tecnologías de la Información y Comunicación y Analista de Soporte Técnico, en base a un documento estructurado de 11 preguntas información que fue requerida para conocer la realidad actual de la infraestructura del "Hospital General Alfredo Noboa Montenegro", en base a esta información recolectada se dio inicio a una elección de las herramientas de escaneo de las cuales se eligió 3 herramientas como son: NESSUS, NMAP y RAPID7 con la finalidad de realizar un escaneo minucioso a la infraestructura y detectar las posibles amenazas y vulnerabilidades a las que están expuestos sus activos existentes, adicional se realizó una valoración de criticidad e impacto de los riesgos basado en la metodología de MAGERIT y conceptos de la norma ISO 27001.

3.5. Procesamiento de la información y análisis estadístico:

Se realizo un levantamiento de información a través de la entrevista y encuesta aplicada al personal de área de tecnologías de información, así como de las pruebas de monitoreo de red con ayuda de las herramientas de escaneo donde se realizó un análisis de los datos relevantes que permitieron demostrar las amenazas y debilidades a las que se encuentra expuesto la infraestructura de red actual, y que procesos y políticas de mejora se pueden implementar a partir de estos datos para tener un gestión eficiente

de la seguridad informática aplicada a los activos tecnológicos existentes en el "Hospital General Alfredo Noboa Montenegro".

Para el desarrollo del proyecto de investigación se realizó las siguientes actividades:

- Revisión de la información recopilada. (encuesta y entrevista a personal del área de TI).
- Análisis e interpretación de los datos de amenazas y vulnerabilidades que se obtuvo del escaneo con la ayuda de las herramientas de escaneo.
- Interpretación de la información relevante que contribuya al desarrollo del proyecto de investigación que lleve a la solución de la propuesta.
- Planteamiento de la propuesta de solución.
- Elaboración de un procedimiento que permita gestionar de una manera eficiente la seguridad perimetral en el área de tecnologías del "Hospital General Alfredo Noboa Montenegro"

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Resultados Pre- implementación.

La recopilación de información sobre aspectos importantes de seguridad informática, se inició con una entrevista compuesta por 11 preguntas respecto aspectos importantes de seguridad a los encargados de la administración del área de tecnologías del "Hospital General Alfredo Noboa Montenegro" con la finalidad de conocer la realidad del funcionamiento y parámetros básicos de seguridad de los equipos tecnológicos como routers, switch, servidores, etc. Anexos II, III.

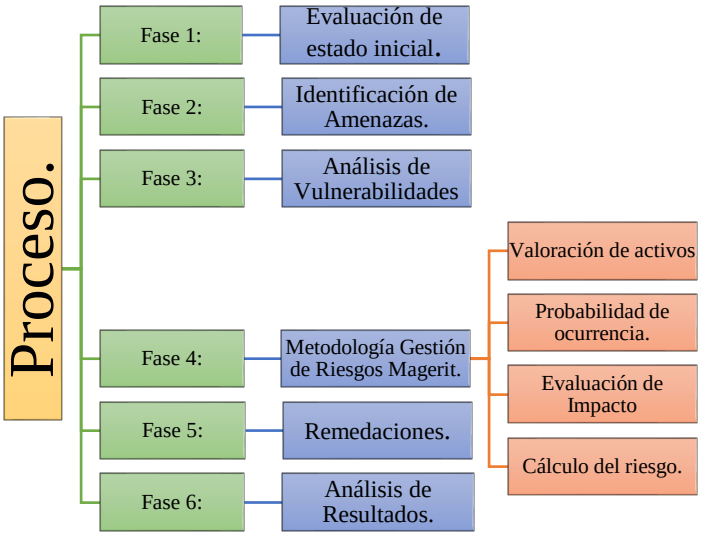
4.2. Evaluación de la seguridad informática perimetral en la infraestructura de una organización, mediante normas y metodologías de seguridad.

Este trabajo de investigación se desarrolla en base a un método cualitativo fundamentado en la recopilación de información, a partir de un caso específico como es la seguridad informática perimetral en la infraestructura de red del "Hospital General Alfredo Noboa Montenegro" estudio que tiene como objetivo recomendar un procedimiento de gestión de la seguridad informática que cumpla con los requisitos de seguridad.

Para cumplir con el propósito del presente estudio, se diseñó una metodología o proceso para la evaluación e implementación medidas correctivas y preventivas que ayuden con la validación del proceso empleado, es importante tener en cuenta que la evaluación del proceso se fundamentara en la aplicación de la normativa ISO/IEC 27001-2013

Figura 16

Procedimiento para la evaluación de la seguridad informática.



Nota. La figura muestra como está estructurado el proceso para el desarrollo del proyecto de investigación. Elaborado por (D. Peña, 2023).

Para el desarrollo del estudio de investigación, se realizó una revisión de la situación actual de la institución "Hospital General Alfredo Noboa Montenegro" en relación a la seguridad informática perimetral que cuenta su infraestructura de datos, se realizó los siguientes pasos teniendo como referencia los conceptos de la norma ISO/IEC 27001:

1. Revisión de Información: lectura de documentos, políticas, normas y procedimientos relacionados a la seguridad informática en la institución. Cabe indicar que la institución empleaba las normas ITIL, desarrollada por el Ministerio de Telecomunicaciones para registros e informes de incidentes de seguridad.
2. Análisis si cuenta con un procedimiento de políticas y procedimientos relacionados con la protección de la información de sus activos tecnológicos y de datos.
3. Evaluación de su infraestructura tecnológica tales como redes, routers, swtichs, servidores, etc. La administración de sus equipos, estándares de seguridad y registro de detección de vulnerabilidad o puntos débiles presentes o que fueron solucionados.

4. Controles de seguridad: se examinó los controles implementados en la institución como cortafuegos, detección de intrusos y políticas de acceso, adicional se verifico que la institución contrata un servicio de firewall por terceros que es administrado por el proveedor CNT, que garantiza la seguridad de su información.
5. Gestión de Datos: se evidencio que para los respaldos de almacenamiento la institución asigna cuentas a cada usuario en la nube, pero que son administrados específicamente por el dueño de la cuenta para su almacenamiento, respaldo y eliminación de datos e información es decir el personal de la institución es responsable de su información.
6. Revisión de Incidentes: cuenta con protocolos de atención de incidentes de seguridad y medidas de reacción para mitigar el impacto de estos eventos.
7. Cumplimiento Normativo: personal del área de tecnologías tiene conocimiento de normas legales y requisitos de protección de datos, pero la institución por falta de presupuesto no ha adquirido una certificación para mejorar y fortalecer sus sistemas de comunicación y resguardo de datos.

4.3. Descripción de la metodología.

Con la finalidad de lograr un proceso metodológico eficiente y aplicable para la institución "Hospital General Alfredo Noboa Montenegro", se ha optado por utilizar herramientas para el escaneo de vulnerabilidades y la ejecución de la metodología de MAGERIT para la valoración y criticidad de sus activos, análisis que permitirá en base a sus resultados adaptarle a conceptos básicos de la norma ISO/IEC 27001, para el tratamiento de riesgos y la posibles mejorar a implementar en base a las deficiencias de seguridad informática identificadas.

4.3.1. Fase 1: Evaluación del estado inicial.

4.3.1.1. Definición de alcance.

El desarrollo del estudio de investigación en la institución "Hospital General Alfredo Noboa Montenegro" tiene como objetivo la aplicación de la siguiente metodología con la finalidad de fortalecer la seguridad física y lógica de sus activos existentes empleando políticas y normas de calidad que permitan garantizar la confidencialidad, integridad y disponibilidad de su información de datos.

4.3.1.2. Identificación de activos.

En base a una investigación en el área de tecnología TI del "Hospital General Alfredo Noboa Montenegro", se procede a identificar los activos más importantes en la institución, se elaboró un inventario general de equipos tecnológicos de la infraestructura de red, información que se recopilo en base a la tabla 2, con la siguiente información de cada activo, equipo, marca, modelo, precio, capacidad, sistema operativo y principales características de cada uno.

Tabla 2

Inventario de Activos de la institución HGANM.

EQUIPOS TECNOLOGICOS INFRAESTRUCTURA DE RED DEL HANM								
ITEM	**EQUIPO**	**MARCA**	**MODELO**	**PRECIO**	**CAPACIDAD**	**DESCRIPCION**	**SO**	**CARACTERISTICAS**
1	Router	Juniper	Juniper Networks SRX650-645AP	$27.600	4 GB	Equipo firewall.	Junos OS 11.2R3	• Interfaces VDSL/ADSL2+ y Ethernet WAN. • 8 puertos LAN Ethernet 10/100. • 2 puertos USB (compatible con USB 3G). • UTM completo; antivirus, antispam, filtrado web mejorado, sistema de prevención de intrusiones, AppSecure. • Control de acceso unificado (UAC) y filtrado de contenidos. • 1 GB de DRAM, 1 GB de flash predeterminado.

2	Smith	Juniper	Juniper Networks EX4200-48T	$8.800	1 GB	Smith para interconexión de equipos	Junos	• 48 puertos 10/100/1000 BASE-T. • 4 puertos 100BASE-FX / 1000BASE-X (SFP) • 2 puertos 10GBASE-X • Velocidad de datos de 136 Gbps • Rendimiento de 101 Mbps (velocidad de cable) • 24.000 direcciones MAC • 4.096 VLAN • 12.000 unidifusión IPv4, 2.000 rutas de multidifusión • Fuente de alimentación DC.
3	Servidor	Fujitsu	Fujitsu Primergy BX400 S1	$9.467,84	20 T	Equipo almacenamiento página web.	Linux Mint 19.3 PHP 7.2	• 2 procesadores Intel Xeon E5-2640V3 de 2,60 GHz. • 8 memorias DDR4 2133 de 16 GB. • Almacenamiento - 2 bahías SAS de 2,5". • 2 x CB Eth Switch/IBP 10Gb. • 2 x BX900 Management Blade S1. • 2 puertos LAN de servicio dedicado Ethernet de 1 Gb para MMB.
4	Controlador	Mitel	3300 CX II	$695,00	1 GB	Sistema de conmutación VoIP.	Mitel MCD 6.0	• 4 CIM, T1/E1 simple, 4 BRI y DSP II. • Unidad de estado sólido SATA de 16 GB. • 150 dispositivos de conexión. • 2 x ADI 21363 Módulos DSP • 32 supresores de eco AMB. • Canales de compresión G.729a (DSP II=128, cuatro DSP=32,

								dos DSP=16). • 6 troncales LS. • 4 puertos ONS. • 64 canales E2T. • STP y RSTP.
5	Router	Cisco	1941 series	$3195,00	512 MB	Interconexión, reglas y protocolos de enrutamiento.	Cisco IOS	• 2 puertos Ethernet 10/100/1000 integrados: GE0/0 y GE0/1 • 2 ranuras para tarjetas de interfaz WAN de alta velocidad giga. • 1 ranura para módulo de servicios internos. • Protocolo de enrutamiento: OSPF, IS-IS, BGP, EIGRP, DVMRP, PIM-SM, IGMPv3, GRE, PIM-SSM, static IPv4 - IPv6. • Gestión remota SNMP, RMON. • Estándares IEEE 802.3ah, IEEE 802.1ah, IEEE 802.1ag. • AC 120/230 V (50/60 Hz).
6	Tranceiver	Humanity	HM-T1000B	$95,00	10/100/1000 M (velocidad)	Transmisión ethernet a través de Fibra Óptica.	N/A	• Estándares de IEEE802.3, IEEE 802.3.u. • Adaptación automática full/half dúplex. • Autoadaptación 10/100/1000M. • 1 puerto ethernet. • Conector: SC predeterminado, opción SC/FC/LC. • Distancia 20 km, 1310 nm. • Conector: RJ45. • Control de flujo de soporte.
								• 24 puertos básicos de conmutación RJ-45.

7	Switch	Cisco	Catalyst 2960	$4.779,00	128 MB	Acceso LAN conectividad y conmutación de redes convergentes	Software IOS 12.2	• 4 puertos SFP/SFP+. • Conectividad Alámbrico. • Ruteo de IP. • Soporte de control de flujo. • IGMP, RMON, SNMP, Telnet, Radius. • 32 Gbit/s capacidad de conmutación. • 12000 entradas direcciones físicas MAC. • 100-240 VAC, 8.0-4.0A, 50-60Hz
8	Catalizador	Cisco	Catalyst 3560E-12D	$1.476,92	256 MB	Conmutadores multicapa de agregación y acceso independientes para aplicaciones convergentes seguras.	Servicios IP de Cisco IOS	• 12 puertos 10 GE. • Aplicaciones como telefonía IP, conexión inalámbrica y video. • Protocolo de gestión remota SNMP 1, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c • Utilización de backplane 2:1 con sobresuscripción. • Modo de comunicación Half-dúplex, full-dúplex. • Velocidad de transferencia de datos 10 Gbps.
9	Tranceiver	Tp-Link	MC111CS	$70,00	10/100 M (velocidad)	Transmisión ethernet a través de Fibra Óptica	N/A	• Estándares de IEEE802.3, IEEE 802.3.u. • Adaptación automática full/half dúplex. • Autoadaptación 10/100 M. • 1 puerto ethernet. • Conector: SC predeterminado, opción SC/FC/LC. • Distancia 20 km, 1310 nm. • Conector: RJ45.
								• Estándares de IEEE802.3,

10	Tranceiver	Tp-Link	MC200CM	$85,00	10/100/1000 M (velocidad)	Transmisión ethernet a través de Fibra Óptica	N/A	IEEE 802.3.u. • Adaptación automática full/half dúplex. • Autoadaptación 10/100/100 M. • 1 puerto ethernet. • Conector: SC predeterminado, opción SC/FC/LC. • Distancia 20 km, 1310 nm. • 2 hilos ópticos Tx – Rx.
11	Servidor	Fujitsu	Fujitsu Primergy RX200 S6	$1478,86	32 GB	Servidor gestión ocupación de camas HANM.	CentOS 7 PHP 5.6 MYSQL 5.5	• 1 ranuras x4 PCI Express. • 2 ranuras x8 PCI Express • Fuente de alimentación conectable en caliente con 92 % de eficiencia. • Hexa-Core (6 núcleos). • CPU 2x Intel XEON X5660 6C 2,80GHz. • 2 puertos VGA (D-Sub). • 1 puerto serial. • 6 puertos USB 2.0. • 2 Ethernet LAN (RJ-45) cantidad de puertos. • 192 GB memoria interna máxima. • Conexión Gigabit Ethernet.
							Linux Mint 19.3 PHP	• 4 puertos Ethernet 10/100/1000 Base-T. • 1 puerto Ethernet 10/100Base-T dedicado. • 8 unidades de disco sólido de 32 GB. • 100-200 V / 200-240 V CA (50-60 Hz). • Uno o dos Dual-Core o Quad-Core. • Procesadores AMD Opteron. • Una unidad EIDE DVD+/-

12	Servidor	Sunfire	X4140	$2318,37	128 GB	Servidor gestión ocupación de camas HANM.	7.2 Postgres 10	RW. • Soporta software como Solaris, Linux, VMware ESX 3.0.2, Windows 2003, etc. • 16 ranuras DIMM DDR2. • Admite desde 2 GB (2 de 1 GB) hasta 64 GB (16 de 4 GB) de memoria. • Un puerto RJ45 asíncrono TIA/EIA-232-F.
13	UPS	Emerson	Liebert GXT3	$1,090.00	1500 VA	Respaldo de energía para servidores y equipos de comunicación.	Sistema de supervisión Vertiv Nform™	• Transformador de aislamiento de salida que permite tensiones de 110/120 fase a neutro o 208/220 entre fases. • Aplicables para Servidores LAN y WAN, equipos de red, telefonía IP, equipos controlados por microprocesadores, RDSI y Frame Relay, etc. • Se pueden poner en paralelo hasta 3 unidades (2+1). • Puerto de comunicación Vertiv IntelliSlot. • Comunicación a través de puerto USB. • Apagado de emergencia (EPO). • Tensión 220/230/240VAC.
14	Monitoreo	AKCP	Probe-5E	$1.090,00	2 GB	Vigilancia de habitaciones de alta	Linux	• 4 puertos de video USB 2.0 MJPEG. • 1 puerto de módem USB 2.0. • Altavoz de micrófono / audio. • 8 puertos AutoSense RJ-45 completos. • 2 puertos de expansión RJ-45. • SNMP V3, correo electrónico, SMS, MMS.

	Remoto					gama		• sensor de temperatura / humedad. • Fuente de alimentación interna. • Temperatura: Mín. -35 ° C - Máx. + 55 ° C • Humedad: Mín. 20% - Máx. 80% (sin condensación) • Energía 3375 vatios, 0,45 A.

Nota. La tabla detalla los activos existentes en la infraestructura de red del “Hospital General Alfredo Noboa Montenegro”

Activos de la Institución "Hospital General Alfredo Noboa Montenegro.

Para validar la metodología empleada en el desarrollo de la propuesta, se ha contado con la colaboración de la institución gubernamental "Hospital General Alfredo Noboa Montenegro" en la provincia Bolívar específicamente en el cantón Guaranda. La disposición de la institución especialmente de sus autoridades y la colaboración del personal de área de TICS encargados como el Ing. Raúl Camacho, analista de TICS y Ing. Wilmer Quicaliquin, analista de Soporte de TICS, para la identificación de activos y equipos de administración de red con los que cuenta la institución fueron importantes para obtener la información necesaria para el desarrollo del trabajo de titulación.

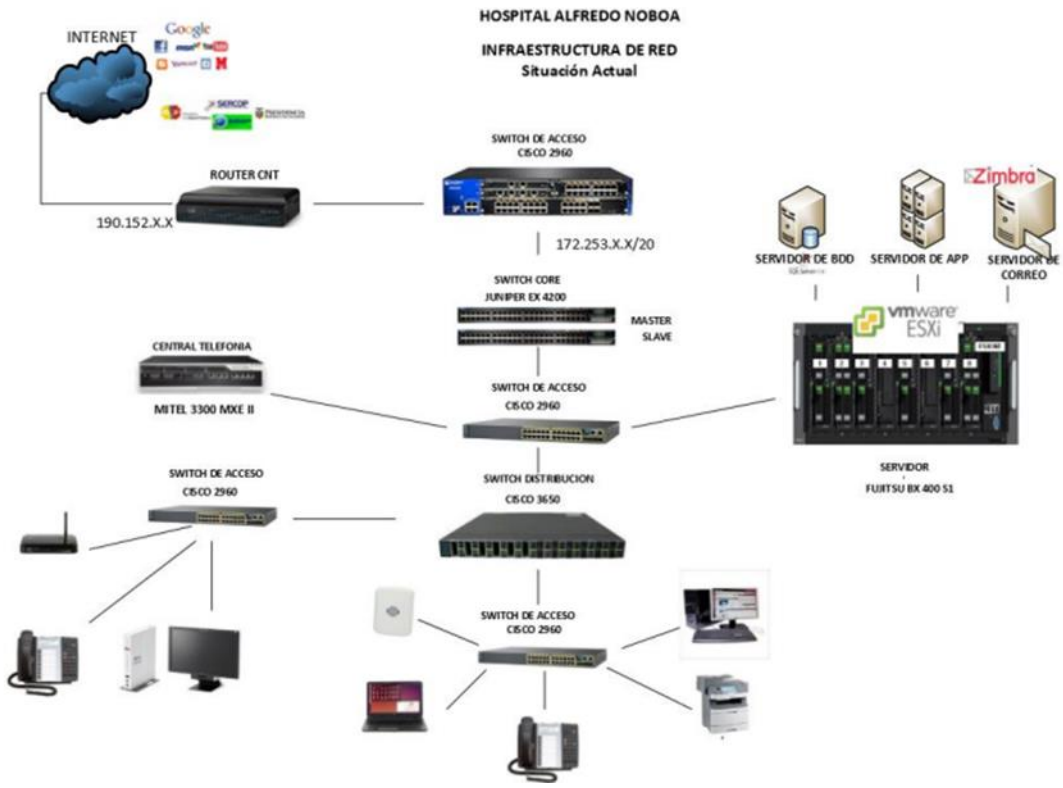
A la fecha de presentación de este proyecto, se cuenta con los siguientes equipos:

- *2 router.*
- *2 centrales telefónicas*
- *4 servidores.*
- *6 switch.*
- *1 sistema de monitoreo.*
- *3 computador de escritorio.*
- *4 teclados.*
- *2 aire acondicionados.*
- *Respaldo de baterías.*
- *2 cámaras IP.*
- *1 sistema de acceso al datacenter.*
- *2 tranceivers de fibra óptica.*

De acuerdo a la información obtenida con la investigación de campo, la infraestructura de red de la institución “Hospital General Alfredo Noboa Montenegro” está diseñada de la siguiente manera, como se muestra en la figura 17.

Figura 17

Infraestructura de red existente en el HGANM.



Nota. La figura muestra el diseño y estructuración de la infraestructura tecnológica del “Hospital General Alfredo Noboa Montenegro”. Elaborado por (D. Peña, 2023).

4.3.2. Fase 2: Identificación de amenazas

Mediante la información obtenida de los activos existentes en el "Hospital General Alfredo Noboa Montenegro" se detalla las posibles amenazas a las cuales esta expuestos y podrían afectar la seguridad de los activos de información, puede ser mediante factores internos y externos, como se observa en las tablas 3,4,5,6.

Tabla 3

Posibles amenazas activos de hardware.

Tipo de Activo	Amenaza
Hardware	Fuego
	Perdida de equipo.
	Falla energía eléctrica.
	Acceso no autorizado.
	Terremoto
	Errores de configuración.
	Manipulación de equipos
	Inundaciones
	Fallas de Fabrica.
	Ataques Informáticos.

Nota. La tabla muestra las amenazas que pueden estar expuestos los activos de Hardware.

Tabla 4

Posibles amenazas activos de Software.

Tipo de Activo	Amenaza
Software	Falla de actualizaciones.
	Difusión de software dañino.
	Errores de usuarios.
	Falta de licencia.
	Falta de mantenimiento
	Manipulación de programas
	Infección por Virus/Malware
	Almacenamiento inadecuado
	Software no compatible.

Nota. La tabla muestra las amenazas que pueden estar expuestos los activos de Software.

Tabla 5

Posibles amenazas activos de Personal.

Tipo de Activo	Amenaza
Personal	Fugas de información.
	Extorsión.
	Indisponibilidad.
	Ingeniería Social.

Nota. La tabla muestra las amenazas que pueden estar expuestos los activos de Personal.

Tabla 6

Posibles amenazas otros activos.

Tipo de Activo	Amenaza
Otros	Fuego.
	Fallas de fábrica.
	Daños por agua.
	Falta suministro eléctrico.
	Equipos obsoletos

Nota. La tabla muestra las amenazas que pueden estar expuestos otros activos.

4.3.3. Fase 3: Análisis de vulnerabilidades.

El análisis de vulnerabilidades en el campo de la seguridad informática es muy importante al momento de prevenir incidentes de seguridad, reducción de costos a largo plazo, así como la concientización de las instituciones al momento de proteger su infraestructura tecnológica, datos y un tratamiento adecuado a amenazas y vulnerabilidades que se pueden detectar.

El “Hospital General Alfredo Noboa Montenegro” tiene como objetivo tener una arquitectura de seguridad informática que proteja y garantice la integridad de sus activos y protección de su información, por lo que se va utilizar las siguientes metodologías con la finalidad de detectar las posibles vulnerabilidades existentes en su infraestructura:

- PTES (Penetration Testing Execution Standard).
- OSSTMM (Open-Source Security Test Methodology).

Para realizar la detección de vulnerabilidades se eligió las siguientes herramientas de escaneo en tiempo real, como muestra la tabla 7.

Tabla 7

Comparación de las herramientas Rapid7, Nessus y NMAP.

Características	Rapid7	NMAP	Nessus
Licencia	✓ Comercial. ✓ Gratuita.	✓ Gratuita.	✓ Comercial. ✓ Gratuita.
Gestión de vulnerabilidades.	✓ Si.	✓ Si.	✓ Si.
Escaneo de red.	✓ Si.	✓ Si.	✓ Si.
Integración API.	✓ Si.	✓ Si.	✓ Si.
Escaneo de aplicaciones.	✓ Si.	✓ Si.	✓ Si.
Compatibilidad.	✓ Multiplataforma.	✓ Multiplataforma.	✓ Multiplataforma.
Escaneo en la Nube.	✓ Si.	✓ No.	✓ Si.
Base de datos de vulnerabilidades.	✓ Si.	✓ Si.	✓ Si.
Reporte avanzado	✓ Si.	✓ Si.	✓ Si.
Soporte Técnico	✓ Si.	✓ Si.	✓ Si.

Nota. La tabla muestra un análisis de comparación de las herramientas de escaneo de vulnerabilidades.

4.3.3.1.Pruebas de escaneo NESSUS.

Es una aplicación que permite el escaneo de vulnerabilidades, debido a su interfaz gráfica amigable se ha convertido en la más utilizada con la finalidad de identificar y evaluar posibles debilidades de los sistemas en la infraestructura de redes, encontrando sus análisis de una forma detallada de sus vulnerabilidades lo que permite a los administradores de red tomar soluciones eficientes en el campo de seguridad de su red de datos.

La aplicación cuenta con 3 opciones para su utilización:

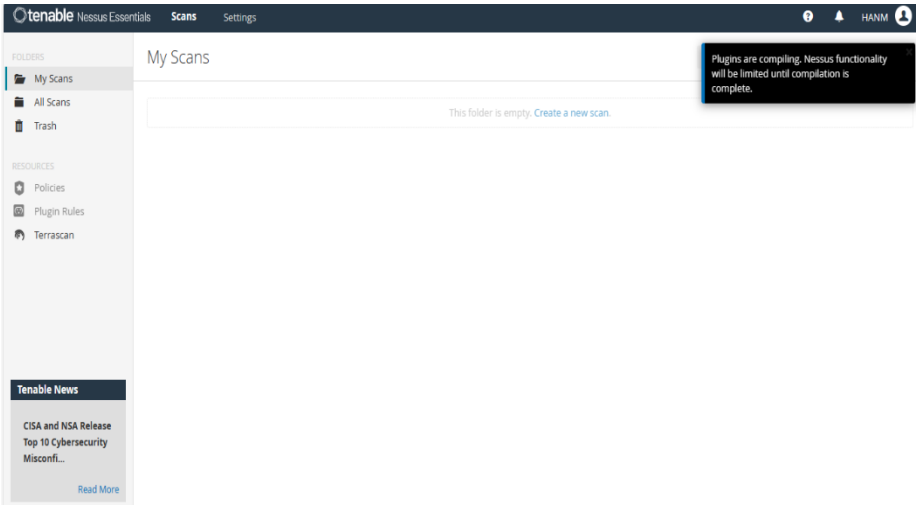
- ✓ Nessus Essentials, que permite el análisis de hasta 16 activos de forma gratuita.
- ✓ Nessus PRO, adecuado para consultores y expertos en seguridad.
- ✓ Tenable.io, diseñado para empresas y gestión de vulnerabilidades.

Para el presente trabajo se utilizó la opción Nessus Essentials, con la finalidad de realizar un análisis profundo de todos los activos existentes de la institución del HGANM, una ventaja es que Nessus es compatible para los sistemas operativos como Linux o Windows.

Una vez culminada la instalación se da inicio al software de Nessus Essentials permitiendo interactuar en su entorno, el mismo que solicita el ingreso del primer lote de sus activos para comenzar con el escaneo de vulnerabilidades, como se observa en la figura 18.

Figura 18

Entono gráfico Nessus Essentials.

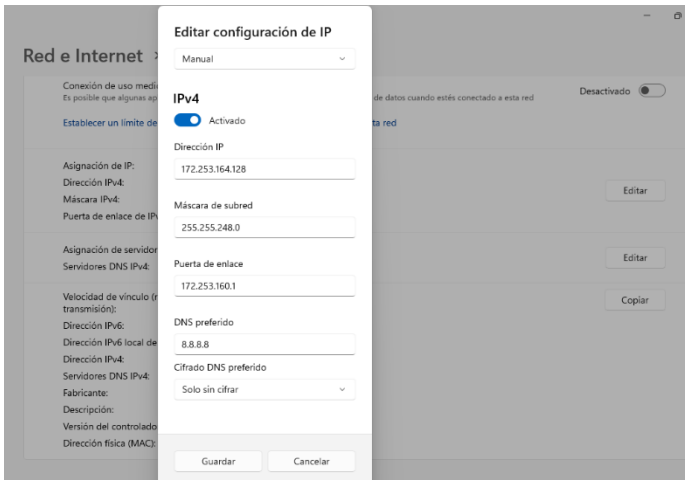


Nota. La figura muestra la interfaz gráfica de la herramienta NESSUS.

Para empezar con el escaneo de red se debe configurar nuestro equipo en un rango dentro de la dirección LAN de la red de la institución, ver figura 19.

Figura 19

Configuración de la tarjeta de red de equipo de pruebas.

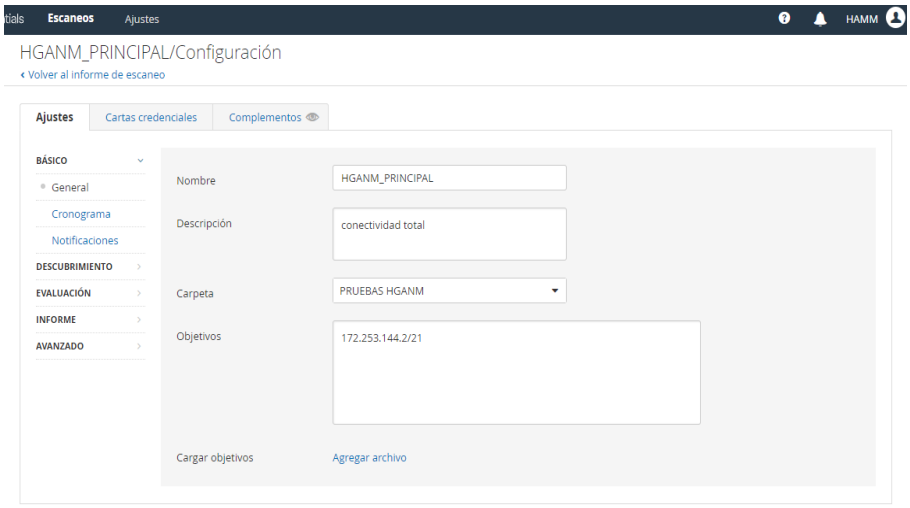


Nota. La figura muestra la configuración de la tarjeta de red del Pc, para iniciar las pruebas.

Se procede a ingresar los activos para comenzar el escaneo de vulnerabilidades, como se muestra en la figura 20.

Figura 20

Ingreso de host 172.253.144.2.

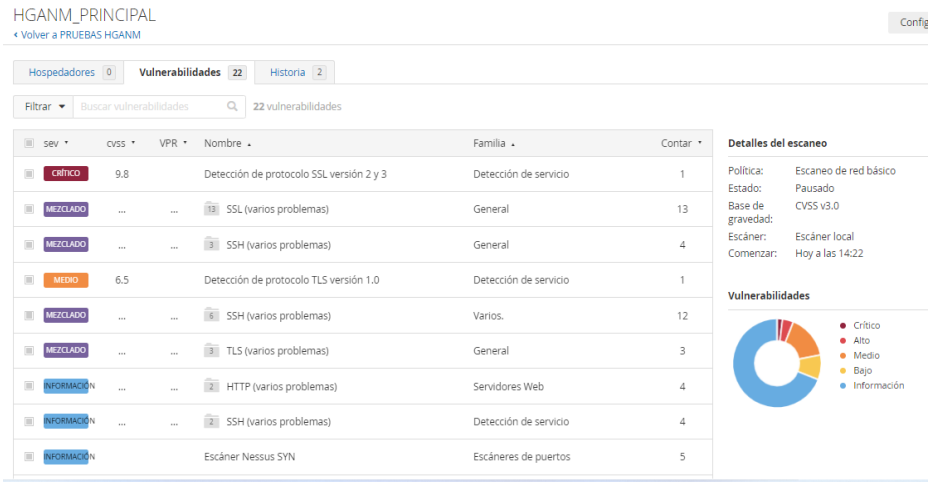


Nota. La figura muestra el ingreso de los activos para el análisis de vulnerabilidades.

En la figura 21, se puede visualizar que se encontró 22 vulnerabilidades en el host 172.253.144.2 entre 4 vulnerabilidades críticas, 5 vulnerabilidades medio y 13 son de tipo informativo.

Figura 21

Vulnerabilidades host 172.253.144.2.

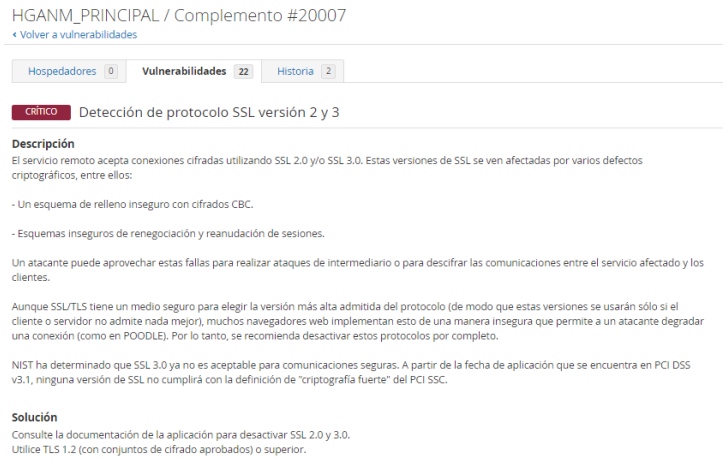


Nota. La figura muestra las vulnerabilidades detectadas en el host 172.253.144.2.

Las vulnerabilidades críticas en el host 172.253.144.2, es por la desactualización del certificado SSL y solución a implementar, muestra la figura 22.

Figura 22

Vulnerabilidad detectada, detalle y solución.



Nota. La figura muestra una vulnerabilidad relacionada al certificado SSL.

El host 172.253.144.2 cuenta con una vulnerabilidad, debido a la utilización del protocolo SSH en la versión 1.33 por lo que se recomienda que se deshabilite la compatibilidad del protocolo SSH, figura 23.

En el Anexo IV se encuentra detallado el análisis de escaneo completo a cada activo del “HGANM”.

Figura 23

Vulnerabilidad detectada, detalle y solución.

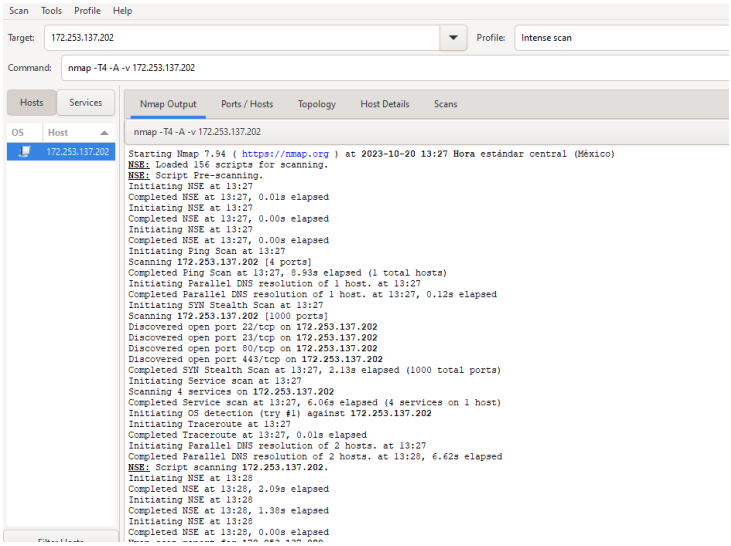
Nota. La figura muestra las soluciones para la vulnerabilidad detectada.

4.3.3.2.Prueba de escaneo NMAP.

Se realiza el análisis a la red 172.253.137.202, del activo de la institución detectando 4 puertos abiertos, como muestra la figura 24.

Figura 24

Análisis de escaneo de la red 172.253.137.202.

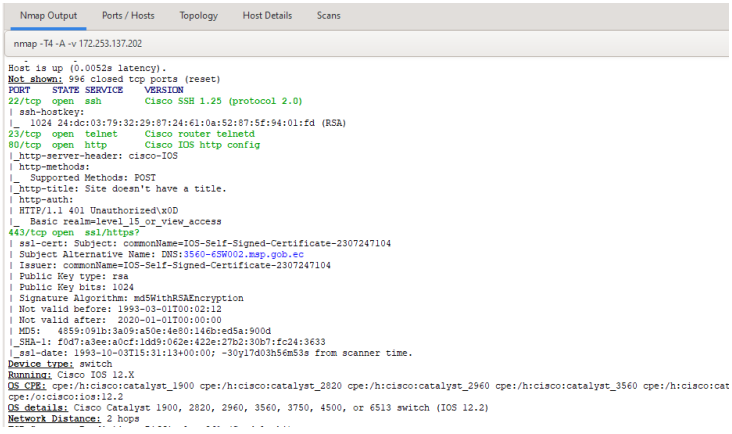


Nota. La figura muestra el escaneo de puertos disponibles en el host.

En la figura 25, de muestra los puertos abiertos de acceso para los protocolos de conexión SSH, HTTP, TELNET, SSL/HTTPS.

Figura 25

Puertos abiertos en la red 172.253.137.202.

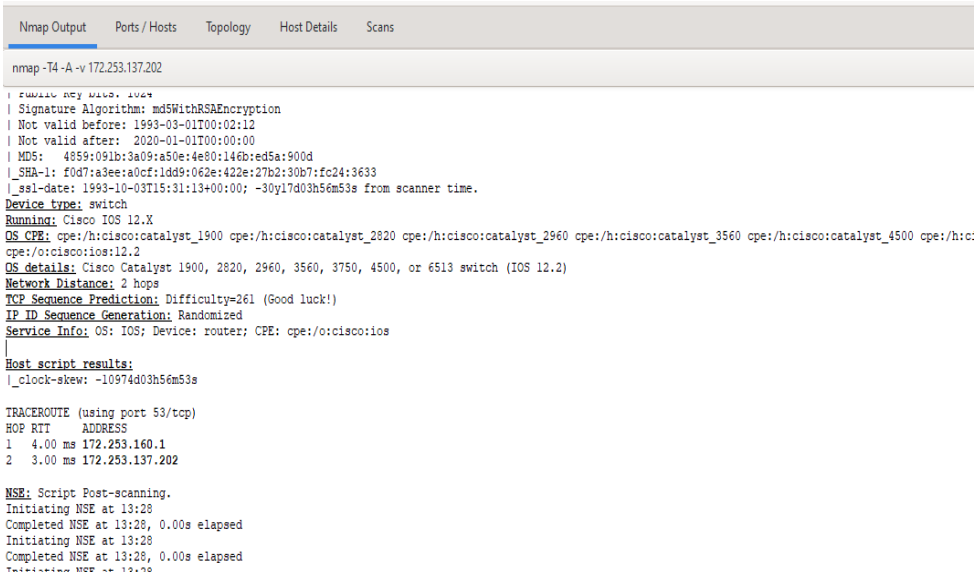


Nota. La figura detalla los puertos abiertos en base a su escaneo en NMAP.

El escaneo mediante NMAP permite visualizar los tiempos de respuesta de transmisión de los paquetes dentro de la red 172.253.137.202, como se observa en la figura 26.

Figura 26

Tiempos de transmisión de paquetes.

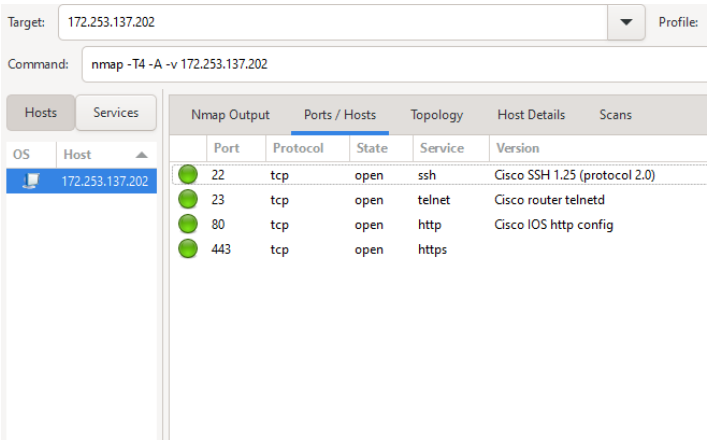


Nota. La figura detalla los tiempos de transmisión de datos.

En el Anexo V se encuentra más a detalle el análisis de cada activo de la institución.

Figura 27

Protocolos y servicios de la red 172.253.137.202.



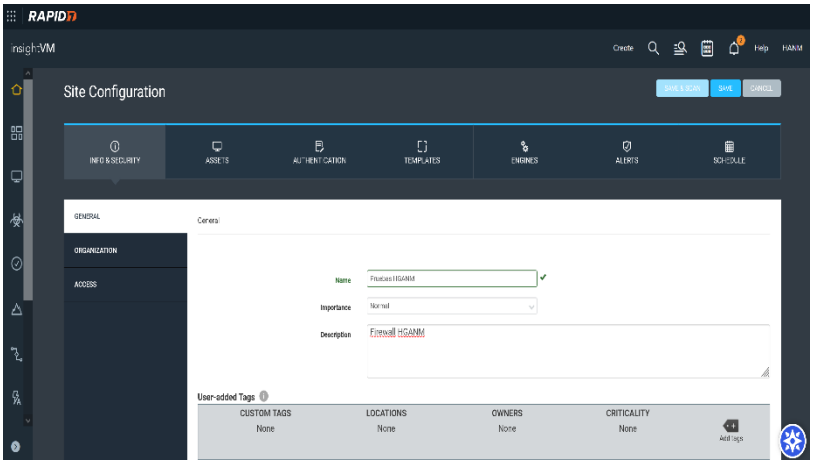
Nota. La figura evidencia de una forma detallada los puertos abiertos disponibles en la red.

4.3.3.3.Pruebas de escaneo Rapid7

Para el análisis de vulnerabilidades de los activos de la institución también se utilizó la siguiente herramienta de escaneo, culminado la instalación y activación del software procedemos a crear un sitio para iniciar las pruebas de escaneo de vulnerabilidades, figura 28.

Figura 28

Crear sitio para inicio de análisis.

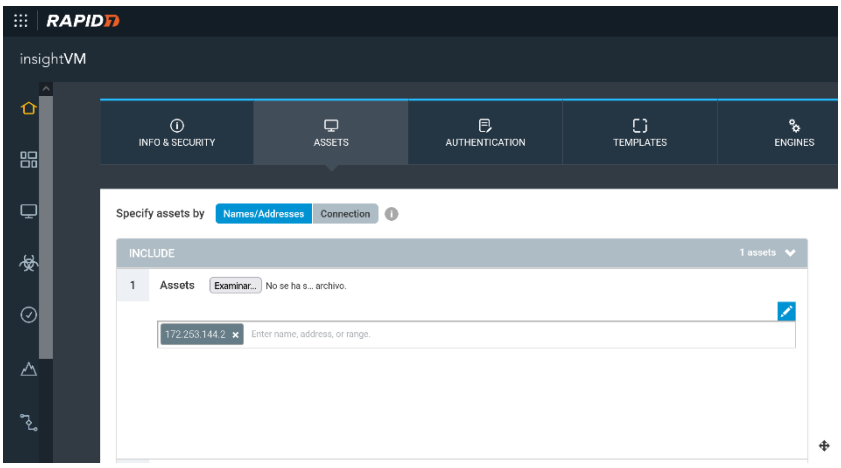


Nota. La figura muestra la creación del sitio en la interfaz de Rapid7.

En la figura 29, se ingresa la IP del host 172.253.144.2 que serán escaneados para la identificación de vulnerabilidades existentes.

Figura 29

Crear de activos de escaneo.

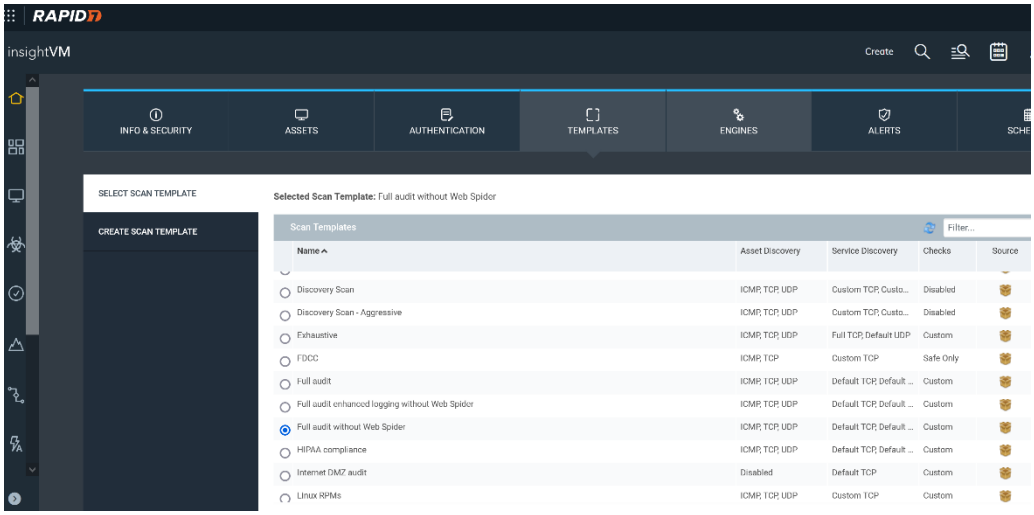


Nota. La figura muestra el ingreso de los activos en el sitio creado en la interfaz.

Se elige la plantilla y tipo para el escaneo a realizarse de los activos ingresados, como se observa en la figura 30.

Figura 30

Elegir el tipo de escaneo a realizar.

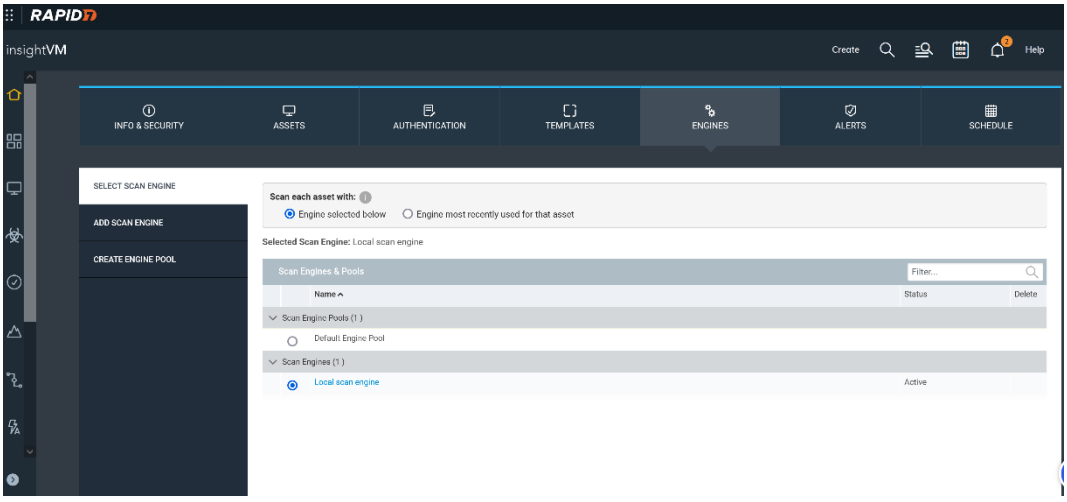


Nota. La figura detalla la elección de tipo de escaneo a realizar en el activo.

Seleccionamos el tipo de motor de escaneo, en este caso sería de tipo local como se selecciona en la figura 31.

Figura 31

Selección de motor de escaneo.

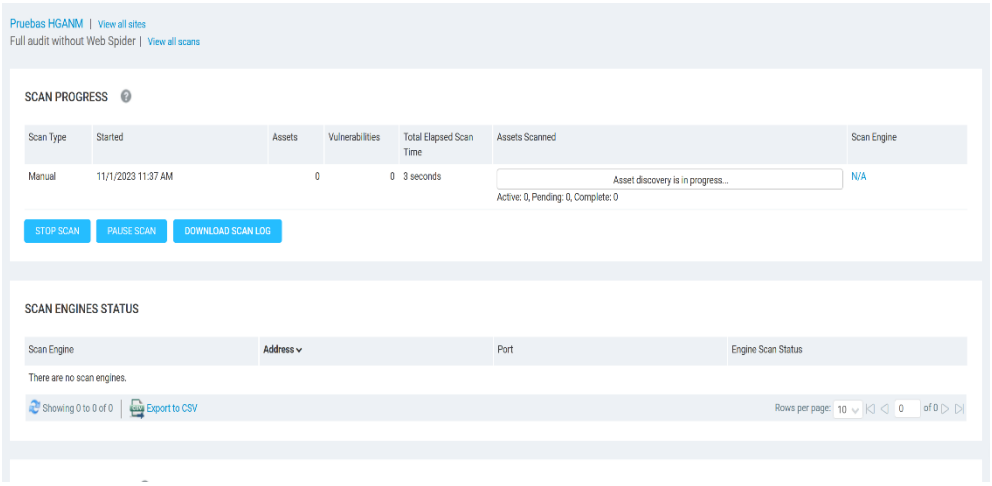


Nota. La figura muestra la configuración del tipo de motor a utilizar en el escaneo de vulnerabilidades.

Se inicia el escaneo de vulnerabilidades para el activo ingresado y configurado en el sitio creado, observar figura 32**.**

Figura 32

Inicio de escaneo de activo.



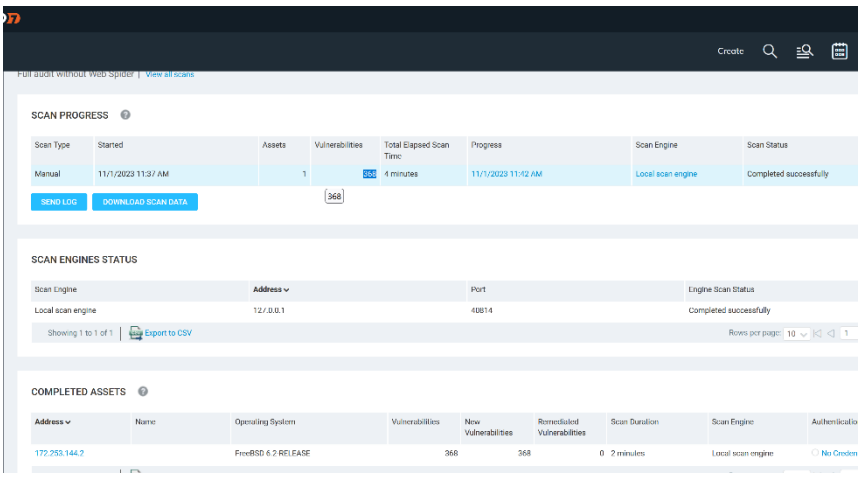
Nota. La figura muestra el progreso del análisis del activo.

Se culmina el escaneo del host 172.253.144.2, donde se detecta 368 vulnerabilidades, como se observa en la figura 33.

En el Anexo VI se encuentra el análisis de escaneo completo a la infraestructura de activos del “Hospital General Alfredo Noboa Montenegro”.

Figura 33

Vulnerabilidades del host 172.253.144.2.



Nota. La figura muestra el número total de vulnerabilidades detectadas en el activo.

4.3.4. Fase 4: Análisis de gestión de riesgos.

En la siguiente fase con la finalidad de cumplir con el desarrollo y la elaboración del Procedimiento de la Gestión de Seguridad Informática para la institución "Hospital General Alfredo Noboa Montenegro" se empleó políticas y controles ya definidos en la Norma ISO 27000 con sus activos, en la cual se realiza el análisis de riesgos utilizando la metodología MAGERIT.

A partir del análisis de riesgos se presenta en la tabla 8, los activos más importantes para la institución gubernamental.

Tabla 8

Clasificación de activos HGANM.

Tipo de activo	Código	Activo
Hardware (HW)	AHW_01	Router Juniper SRX650
	AHW_02	Switch Juniper EX 4200 Series
	AHW_03	Servidor Fujitsu ET08L22AU
	AHW_04	Servidor Pagina web Fujitsu BX400 S1
	AHW_05	Controller VOIP Mitel 3300 CX II
	AHW_06	Router cisco 1941 Series (ISP CNT)
	AHW_07	Switch cisco catalyst 3560 (Interconexión FO)
	AHW_08	Switch cisco catalyst 2960 (subredes)
	AHW_09	Conversor FO Tplink
	AHW_10	Servidor Fujitsu RX200 S6 (gestión camas)
	AHW_11	Servidor Sunfire X4140 (gestión camas)
	AHW_12	Teclado ACCER
	AHW_13	Mouse ACCER
	AHW_14	Monitor HP
	AHW_15	Laptop DELL
	AHW_16	Cámara IP
Tipo de activo	**Código**	**Activo**
Software (SW)	ASW_01	Windows
	ASW_02	Linux Mint 19.3 PHP 7.2
	ASW_03	Software IOS 12.2
	ASW_04	Junos OS 11.2R3
	ASW_05	Centos 7 PHP 5.6 MYSQL 5.5
Tipo de activo	**Código**	**Activo**
Equipos Auxiliares	AAUX_01	Regulador de voltaje
	AAUX_02	Banco de baterías
	AAUX_03	Ups Emerson Liebert GXT3
	AAUX_04	Regleta eléctrica
	AAUX_05	Aire acondicionado Emerson

	AAUX_06	Odf de fibra óptica
	AAUX_07	Rack de equipos
Tipo de activo	**Código**	**Activo**
Personal	AP_01	Analista de Tecnologías de Información
	AP_02	Técnico de Soporte de TICS
Tipo de activo	**Código**	**Activo**
Activos de Información	AD_01	Diagrama de red.
	AD_02	Equipos de respaldo

Nota. La tabla muestra la clasificación de los activos existentes en la institución.

4.3.4.1.Valoración de activos.

La valoración de activos consiste en asignar un valor a cada uno de los activos de la institución de manera cuantitativo o cualitativo, y alinearlo de acuerdo a la metodología propuesta por MAGERIT en lo que respecta a los aspectos de confidencialidad [C], integridad [I], disponibilidad [D], valoración que se tomó como base la escala propuesta en el libro II – Catálogo de Elementos de MAGERIT – versión 3.0, como se muestra en la Tabla 9.

Tabla 9

Criterios de valoración – metodología MAGERIT.

Valor	**Criterios**	
10	Extremo	Daño extremo grave.
9	Muy Alto	Daño muy grave
6 - 8	Alto	Daño grave
3 - 5	Medio	Daño importante
1 - 2	Bajo	Daño menor
0	Despreciable	Irrelevante

Nota. La tabla muestra los criterios de valoración de los activos

Según los criterios de valoración expuestos en la tabla 9, se procedió a valorar los activos del "Hospital General Alfredo Noboa Montenegro" para obtener un promedio en base a la confidencialidad, integridad, disponibilidad.

Para obtener el promedio de la valoración de los activos en los aspectos de confidencialidad, integridad y disponibilidad, se aplicó la siguiente formula

$$P = \frac{C + I + D}{3}$$

Valoración activos Hardware.

Tabla 10

Valoración activos de hardware – MAGERIT CID.

		Dimensiones			Valoración	
Activo	**Ubicación**	**[C]**	**[I]**	**[D]**	**Promedio**	**Valor**
AHW_01	Data center _1	8	8	9	8,33333333	Muy Alto
AHW_02	Data center _1	7	7	8	7,33333333	Alto
AHW_03	Data center _1	7	7	7	7	Alto
AHW_04	Data center _1	7	8	8	7,66666667	Alto
AHW_05	Data center _1	7	7	9	7,66666667	Alto
AHW_06	Data center _2	9	9	9	9	Muy Alto
AHW_07	Data center_2	8	8	9	8,33333333	Alto
AHW_08	Data center_2	8	8	8	8	Alto
AHW_09	Data center_2	5	5	5	5	Medio
AHW_10	Data center_2	7	8	9	8	Alto
AHW_11	Data center_2	7	8	9	8	Alto
AHW_12	Data center_2	6	7	7	6,66666667	Alto
AHW_13	Data center_2	5	5	5	5	Medio
AHW_14	Data center_2	5	5	5	5	Medio
AHW_15	Data center_2	8	8	10	8,66666667	Muy Alto
AHW_16	Data center_2	7	9	9	8,33333333	Muy Alto

Nota. La tabla muestra la valoración de los activos de Hardware.

Tabla 11

Valoración activos de software – MAGERIT CID.

		Dimensiones			Valoración	
Activo	**Ubicación**	**[C]**	**[I]**	**[D]**	**Promedio**	**Valor**
ASW_01	Área de soporte.	8	8	10	8,66666667	Muy alto
ASW_02	Área de soporte.	8	8	8	8	Alto
ASW_03	Área de soporte.	7	6	7	6,66666667	Alto
ASW_04	Área de soporte.	5	5	5	5	Medio
ASW_05	Área de soporte.	8	7	7	7,33333333	Alto

Nota. La tabla muestra la valoración de los activos de Software.

Tabla 12

Valoración activos equipos auxiliares – MAGERIT CID.

		Dimensiones			Valoración	
Activo	**Ubicación**	**[C]**	**[I]**	**[D]**	**Promedio**	**Valor**
AAUX_01	Área de soporte.	5	5	5	5	Medio
AAUX_02	Data center_2	8	8	8	8	Alto
AAUX_03	Data center_2	7	7	8	7,33333333	Alto
AAUX_04	Área de TICS	7	7	7	7	Alto
AAUX_05	Data center_1	7	8	8	7,66666667	Alto
AAUX_06	Data Center_2	8	8	9	8,33333333	Muy alto
AAUX_07	Área de TICS	9	9	9	9	Muy alto

Nota. La tabla muestra la valoración de los activos de Equipos Auxiliares.

Tabla 13

Valoración activos personal – MAGERIT CID.

		Dimensiones			Valoración	
Activo	**Ubicación**	**[C]**	**[I]**	**[D]**	**Promedio**	**Valor**
AP_01	Área de TICS	9	9	9	9	Muy alto
AP_02	Área de TICS	8	8	8	8	Alto

Nota. La tabla muestra la valoración de los activos personal.

Tabla 14

Valoración de activos información. – MAGERIT CID.

		Dimensiones			Valoración	
Activo	**Ubicación**	**[C]**	**[I]**	**[D]**	**Promedio**	**Valor**
AD_01	Área de TICS	8	8	8	8	Alto
AD_02	Área de TICS	7	7	7	7	Alto

Nota. La tabla muestra la valoración de los activos de información.

4.3.4.2. Probabilidad de Ocurrencia.

Para la identificación de vulnerabilidades y amenazas se tomó como base la lista de amenazas que se describen en el libro II – Catálogo de Elementos de MAGERIT –

versión 3.0 y en base a los activos existentes en el área de tecnologías del "Hospital General Alfredo Noboa Montenegro" se procedió a crear una escala de valoración para la degradación y probabilidad de ocurrencia, como se muestra en la Tabla 15.

Tabla 15

Criterios de valoración de amenazas.

Valor	Degradación	Probabilidad de Ocurrencia
10	Extremo	Diario
9	Muy Alto	Varias veces a la semana
6 - 8	Alto	1 vez al mes
3 - 5	Medio	1 vez al año
1 - 2	Bajo	Rara vez
0	Despreciable	Irrelevante

Nota. La tabla muestra los criterios de valoración de probabilidad de ocurrencia.

Finalmente, con la escala de valoración de las amenazas por degradación y probabilidad de ocurrencia, se procedió a realizar mediante un análisis la probabilidad de que una amenaza se materialice en los activos existentes en la institución.

Tabla 16

Probabilidad de ocurrencia activos software.

Activo	Vulnerabilidad	Amenaza	Degradación	P. Ocurrencia
ASW_01	Software no documentado.	Errores de software.	7	6
ASW_02	Compartición de archivos infectos.	Código malicioso.	8	6
ASW_03	Ausencia de sistemas de identificación y autenticación.	Acceso no autorizado.	7	5
ASW_04	Claves de acceso comprometidas.	Errores de administración.	6	4
ASW_05	Ausencia de sistemas de identificación y autenticación.	Instalación no autorizada de software.	3	2

Nota. La tabla muestra la probabilidad de ocurrencia activos de Software.

Tabla 17

Probabilidad de ocurrencia activos hardware.

Activo	Vulnerabilidad	Amenaza	Degradación	P. Ocurrencia
AHW_01	Susceptible a variaciones de tensión o voltaje.	Falla de energía eléctrica.	3	7
AHW_02	Falla funcionamiento de equipo.	Falta de Mantenimiento Preventivo.	8	5
AHW_03	Falla funcionamiento de equipo.	Ataques informáticos.	9	6
AHW_04	No tener inventario de activos	Perdida de equipos.	6	1
AHW_05	Falla de configuración de equipo.	Errores de actualización de equipos.	6	4

AHW_06	Falla de interconexión de equipos.	Caída del proveedor de internet.	1	5
AHW_07	Fallas instalaciones eléctricas.	Fuego.	7	1
AHW_08	Software no documentado	Errores de software.	9	6
AHW_09	Mantenimiento inadecuado.	Mal funcionamiento del equipo.	8	4
AHW_10	Falta de control de acceso.	Ingreso no autorizado al equipo.	3	2
AHW_11	Falta de conocimientos del administrador de equipos.	Errores de administración.	7	5
AHW_12	Remplazo inadecuado de equipos viejos.	Mal funcionamiento del equipo.	6	3
AHW_13	Manipulación errónea de los periféricos.	Errores de los usuarios.	10	8
AHW_14	Fallas en los componentes electrónicos internos.	Avería de origen físico o lógico.	7	4
AHW_15	Ingresar a los equipos de la organización sin previo aviso o autorización.	Acceso no autorizado.	10	9
AHW_16	Desprotección en equipos de vigilancia.	Daño causado por un tercero.	5	2

Nota. La tabla muestra la probabilidad de ocurrencia activos de Hardware.

Tabla 18

Probabilidad de ocurrencia activos auxiliares.

Activo	Vulnerabilidad	Amenaza	Degradación	P. Ocurrencia
AAUX_01	Falla en instalaciones eléctricas	Fuego.	6	3
AAUX_02	Mantenimiento inadecuado.	Perdida de respaldo de energía.	4	3
AAUX_03	Mantenimiento inadecuado.	Mal funcionamiento del equipo.	8	4
AAUX_04	Falla en los componentes eléctricos.	Avería de origen físico.	9	5
AAUX_05	Fallas en los componentes electrónicos internos.	Avería de origen físico y lógico.	3	2
AAUX_06	Intermitencia de transmisión.	Manipulación de FO.	2	1
AAUX_07	Falta de documentación interna.	Acceso físico no autorizado.	7	3

Nota. La tabla muestra la probabilidad de ocurrencia activos auxiliares.

Tabla 19

Probabilidad de ocurrencia activos personal.

Activo	Vulnerabilidad	Amenaza	Degradación	P. Ocurrencia
AP_01	Respaldos inapropiados.	Perdida de Información.	1	5
AP_02	Exceso de carga laboral.	Indisponibilidad	2	4

Nota. La tabla muestra la probabilidad de ocurrencia activos personal.

Tabla 20

Probabilidad de ocurrencia activos gestión de información.

Activo	Vulnerabilidad	Amenaza	Degradación	P. Ocurrencia
AD_01	Inadecuada gestión de la red de datos.	Fallo de enlaces de comunicación.	2	4
AD_02	Clasificación inadecuada de la información.	Fuga de información.	1	5

Nota. La tabla muestra la probabilidad de ocurrencia activos de información.

4.3.4.3.Evaluación de Impacto.

En base a la información recopilada de la institución "Hospital General Alfredo Noboa Montenegro" una vez realizado la identificación de activos, valoración de amenazas y su probabilidad de ocurrencia, es momento de proceder con la evaluación del impacto. Se define como impacto al daño que puede causar sobre el activo al momento de la materialización de una amenaza.

En su estudio Villegas (2009), define que el impacto es la medida del daño o cambio adverso que puede sufrir un activo una vez ya materializada una amenaza.
Para la evaluación del impacto aplicando se va utilizar los criterios de valoración, como se observa en la tabla 21.

Tabla 21

Criterios de Valoración de impacto.

Valor	Criterios	Descripción
10	Extremo [E]	Cuando la amenaza se ha materializado y causa daños relevantes dentro de la organización.
9	Muy Alto [MA]	Cuando la amenaza se ha materializado y causa daños que la institución puede controlar en un periodo largo de tiempo.
6 - 8	Alto [A]	Cuando la amenaza se ha materializado y causa daños que pueden ser controlados en un periodo significativo de tiempo por la institución.
3 - 5	Medio [M]	Cuando la amenaza se ha materializado y los daños son fáciles de controlar en muy poco tiempo por la institución.
1 - 2	Bajo [B]	Cuando la amenaza se ha materializado y los daños ocasionados en la institución no afectan su normal funcionamiento.
0	Despreciable [D]	Una vez materializado la amenaza, no afecta en absoluto al funcionamiento de la organización

Nota. La tabla muestra los criterios de valoración de impacto

Una vez definido la valoración de los criterios de impacto, se procedió a realizar la evaluación de cada uno de los activos existentes en la infraestructura del "Hospital General Alfredo Noboa Montenegro", según su clasificación.

Tabla 22

Valoración de impacto, activos de hardware.

Activo	Vulnerabilidad	Amenaza	Impacto	Criterio
AHW_01	Susceptible a las variaciones de tensión	Falla de energía eléctrica.	8	[A]
AHW_02	Falla funcionamiento de equipo.	Falta de Mantenimiento Preventivo.	8	[A]
AHW_03	Falla funcionamiento de equipo.	Ataques informáticos.	6	[A]
AHW_04	No tener inventario de activos	Perdida de equipos.	9	[MA]
AHW_05	Falla de configuración de equipo.	Errores de actualización de equipos.	7	[A]
AHW_06	Falla de interconexión de equipos.	Caída del proveedor de internet.	9	[MA]
AHW_07	Fallas instalaciones eléctricas.	Fuego.	9	[MA]
AHW_08	Software no documentado	Errores de software.	6	[A]
AHW_09	Mantenimiento inadecuado.	Mal funcionamiento del equipo.	4	[M]
AHW_10	Falta de control de acceso.	Ingreso no autorizado al equipo.	6	[A]
AHW_11	Falta de conocimientos del administrador de equipos.	Errores de administración.	6	[A]
AHW_12	Remplazo inadecuado de equipos viejos.	Mal funcionamiento del equipo.	2	[B]
AHW_13	Manipulación errónea de los periféricos.	Errores de los usuarios.	2	[B]
AHW_14	Fallas en los componentes electrónicos internos.	Avería de origen físico o lógico.	4	[M]
AHW_15	Ingresar a los equipos de la organización sin previo aviso o autorización.	Acceso no autorizado.	4	[M]
AHW_16	Desprotección en equipos de vigilancia.	Daño causado por un tercero.	3	[M]

Nota. La tabla muestra la valoración de impacto de los activos de hardware.

Tabla 23

Valoración de impacto, activos de software.

Activo	Vulnerabilidad	Amenaza	Impacto	Criterio
ASW_01	Software no documentado.	Errores de software.	5	[M]

ASW_02	Pruebas de Software insuficiente.	Código malicioso.	5	[M]
ASW_03	Ausencia de sistemas de identificación y autenticación.	Acceso no autorizado.	6	[A]
ASW_04	Claves de acceso comprometidas.	Errores de administración.	6	[A]
ASW_05	Ausencia de sistemas de identificación y autenticación.	Instalación no autorizada de software.	5	[M]

Nota. La tabla muestra la valoración de impacto de los activos de software.

Tabla 24

Valoración de impacto, activos de equipos auxiliares.

Activo	Vulnerabilidad	Amenaza	Impacto	Criterio
AAUX_01	Falla en instalaciones eléctricas	Fuego.	8	[A]
AAUX_02	Mantenimiento inadecuado.	Perdida de respaldo de energía.	7	[A]
AAUX_03	Mantenimiento inadecuado.	Mal funcionamiento del equipo.	6	[A]
AAUX_04	Falla en los componentes eléctricos.	Avería de origen físico.	3	[M]
AAUX_05	Fallas en los componentes electrónicos internos.	Avería de origen físico y lógico.	6	[A]
AAUX_06	Intermitencia de transmisión.	Manipulación de FO.	4	[M]
AAUX_07	Falta de documentación interna.	Acceso físico no autorizado.	2	[B]

Nota. La tabla muestra la valoración de impacto de los activos de equipos auxiliares.

Tabla 25

Valoración de impacto, activos soporte personal.

Activo	Vulnerabilidad	Amenaza	Impacto	Criterio
AP_01	Respaldos inapropiados.	Perdida de Información.	8	[A]
AP_02	Exceso de carga laboral.	Indisponibilidad	5	[M]

Nota. La tabla muestra la valoración de impacto de los activos de personal.

Tabla 26

Valoración de impacto, activos gestión de información.

Activo	Vulnerabilidad	Amenaza	Impacto	Criterio
AD_01	Inadecuada gestión de la red.	Fallo de enlaces de comunicación.	7	[A]
AD_02	Clasificación inadecuada de la información.	Fuga de información.	5	[M]

Nota. La tabla muestra la valoración de impacto de los activos de información.

4.3.4.4.Cálculo del riesgo.

Consiste en la relación y producto de la probabilidad de ocurrencia y el impacto, para el cálculo del nivel de riesgo de cada amenaza en relación con los activos existentes en la institución.

Tabla 27

Cálculo del riesgo, activos de hardware.

Activo	Vulnerabilidad	Amenaza	P. Ocurrencia	Impacto	Riesgo	Criterio
AHW_01	Susceptible a las variaciones de tensión	Falla de energía eléctrica.	7	8	56	[M]
AHW_02	Falla funcionamiento de equipo.	Falta de Mantenimiento Preventivo.	5	8	40	[M]
AHW_03	Falla funcionamiento de equipo.	Ataques informáticos.	6	6	36	[M]
AHW_04	No tener inventario de activos	Perdida de equipos.	1	9	9	[D]
AHW_05	Falla de configuración de equipo.	Errores de actualización de equipos.	4	7	28	[B]
AHW_06	Falla de interconexión de equipos.	Caída del proveedor de internet.	5	9	45	[M]
AHW_07	Fallas instalaciones eléctricas.	Fuego.	1	9	9	[D]
AHW_08	Software no documentado	Errores de software.	6	6	36	[M]
AHW_09	Mantenimiento inadecuado.	Mal funcionamiento del equipo.	4	4	16	[B]
AHW_10	Falta de control de acceso.	Ingreso no autorizado al equipo.	2	6	12	[B]
AHW_11	Falta de conocimientos del administrador de equipos.	Errores de administración.	5	6	30	[M]
AHW_12	Remplazo inadecuado de equipos viejos.	Mal funcionamiento del equipo.	3	2	6	[D]
AHW_13	Manipulación errónea de los periféricos.	Errores de los usuarios.	8	2	16	[B]
AHW_14	Fallas en los componentes electrónicos internos.	Avería de origen físico o lógico.	4	4	16	[B]
AHW_15	Ingresar a los equipos de la organización sin previo aviso o autorización.	Acceso no autorizado.	9	4	36	[M]
AHW_16	Desprotección en equipos de vigilancia.	Daño causado por un tercero.	2	3	6	[D]

Nota. La tabla muestra el cálculo de riesgo de los activos de hardware.

Tabla 28

Cálculo del riesgo, activos de software.

Activo	Vulnerabilidad	Amenaza	P. Ocurrencia	Impacto	Riesgo	Criterio
ASW_01	Software no documentado.	Errores de software.	6	5	30	[M]
ASW_02	Pruebas de Software insuficiente.	Código malicioso.	6	5	30	[M]
ASW_03	Ausencia de sistemas de identificación y autenticación.	Acceso no autorizado.	5	6	30	[M]
ASW_04	Claves de acceso comprometidas.	Errores de administración.	4	6	24	[B]
ASW_05	Ausencia de sistemas de identificación y autenticación.	Instalación no autorizada de software.	2	5	10	[B]

Nota. La tabla muestra el cálculo de riesgo de los activos de software.

Tabla 29

Cálculo del riesgo, activos de equipos auxiliares.

Activo	Vulnerabilidad	Amenaza	P. Ocurrencia	Impacto	Riesgo	Criterio
AAUX_01	Falla en instalaciones eléctricas	Fuego.	3	8	24	[B]
AAUX_02	Mantenimiento inadecuado.	Perdida de respaldo de energía.	3	7	21	[B]
AAUX_03	Mantenimiento inadecuado.	Mal funcionamiento del equipo.	4	6	24	[B]
AAUX_04	Falla en los componentes eléctricos.	Avería de origen físico.	5	3	15	[B]
AAUX_05	Fallas en los componentes electrónicos internos.	Avería de origen físico y lógico.	2	6	12	[B]
AAUX_06	Intermitencia de transmisión.	Manipulación de FO.	1	4	4	[D]
AAUX_07	Falta de documentación interna.	Acceso físico no autorizado.	3	2	6	[D]

Nota. La tabla muestra el cálculo de riesgo de los activos de equipos auxiliares.

Tabla 30

Cálculo del riesgo, activos de soporte personal.

Activo	Vulnerabilidad	Amenaza	P. Ocurrencia	Impacto	Riesgo	Criterio
AP_01	Respaldos inapropiados.	Perdida de Información.	5	8	40	[M]
AP_02	Exceso de carga laboral.	Indisponibilidad	4	5	20	[B]

Nota. La tabla muestra el cálculo de riesgo de los activos de personal

Tabla 31

Cálculo del riesgo, activos de gestión de información.

Activo	Vulnerabilidad	Amenaza	P. Ocurrencia	Impacto	Riesgo	Criterio
AD_01	Inadecuada gestión de la red.	Fallo de enlaces de comunicación.	4	7	28	[B]
AD_02	Clasificación inadecuada de la información.	Fuga de información.	5	5	25	[B]

Nota. La tabla muestra el cálculo de riesgo de los activos de información.

4.3.5. Fase 5: Análisis de Remediaciones de Vulnerabilidades.

En la siguiente fase se concentró en la elaboración de la recomendaciones y posibles correcciones de las vulnerabilidades encontradas en la infraestructura de los activos del "Hospital General Alfredo Noboa Montenegro" con ayuda de las herramientas de escaneo, vulnerabilidades que se encuentran clasificadas de acuerdo a su impacto de afectación, critica, alta, media y baja, para lo cual las remediaciones se enfocaran exclusivamente a las áreas consideradas como puntos vulnerables para los atacantes.

Vulnerabilidades de Software.

Son vulnerabilidades específicas que se presentan en programas instalados, equipos de red y seguridad de software que pueden presentar la infraestructura del "Hospital General Alfredo Noboa Montenegro", provocando fallas e indisponibilidad del servicio en la institución, para lo cual se detalla algunas recomendaciones a tomar en cuenta en la tabla 32.

Tabla 32

Recomendaciones en vulnerabilidades de software.

	Recomendaciones.
Errores de configuración de sistema	• Coordinar mantenimientos periódicos de carácter lógico, para detectar errores de configuración. • No usar software no autorizado o sin licencia. • Actualizar el software, cuando se disponga de actualizaciones y parches disponibles. • Configurar los sistemas de acuerdo a la guía del fabricante.
Gestión deficiente de recursos.	• Emplear los recursos necesarios, mediante la ejecución de tareas que garanticen la efectividad y rendimiento de los activos, ante posibles ataques.

Administración inadecuada de accesos y permisos.	• Establecer normas y políticas para asignación de permisos, según el cargo de empleado, o persona encargada para el soporte o administración de programas y dispositivos de servicio.
Falta de implementación de firewall.	• Se de diseñar e implementar un firewall que garantice la seguridad perimetral de la red.
Expansión de código malicioso.	• Planificar tareas de mantenimiento para actuar en situaciones de emergencia. • Monitoreo de software utilizado y datos de red. • Protección de los dispositivos tecnológicos con antivirus. • Definir responsables para detección de malware.

Nota. La tabla muestra las recomendaciones para vulnerabilidades de software.

Vulnerabilidades de Hardware.

La infraestructura tecnológica de la institución "Hospital General Alfredo Noboa Montenegro", puede presentar varias vulnerabilidades físicas como fallas de hardware, componentes electrónicos y eléctricos, así como estar expuestos a desastres naturales. En la tabla 33 se detalla algunas recomendaciones para controlar estas vulnerabilidades.

Tabla 33

Recomendaciones ante vulnerabilidades de hardware.

	Recomendaciones.
Accesos no autorizados.	• Elaborar políticas de control de acceso, para proteger dispositivos y equipos de la red. • Implementar dispositivos digitales e inteligentes para permitir el acceso de personal a áreas de interacción con dispositivos y equipos tecnológicos.
Falla en componentes de hardware.	• Planificar mantenimientos preventivos y correctivos en componentes tecnológicos como discos duros, memoria RAM, puertos, con la finalidad de prevenir fallas lógicas. • Es recomendable el bloqueo de funcionamiento de los puertos USB, para evitar la expansión de malware o virus informático. • Contar con dispositivos hardware para remplazo ante fallas o vida útil. • Crear un departamento con personal autorizado para mantenimiento de fallas críticas de hardware en equipos.
Desastres Naturales.	• Colocar los equipos en soportes fijos o de goma para evitar caídas ante vibraciones, temblores y terremotos. • Considerar un perímetro adecuado de distancia de ubicación de los equipos con ventanas, banco de baterías o sistemas de climatización, para evitar posibles daños ante cualquier evento. • No colocar objetos móviles sobre dispositivos de red que puedan causar daños al caer sobre ellos. • Diseñar una distribución correcta y ordenada de cables de transmisión de datos, fibra óptica y energía eléctrica.

Nota. La tabla muestra las recomendaciones para vulnerabilidades de hardware.

Vulnerabilidades Humanas.

En la institución "Hospital General Alfredo Noboa Montenegro", cuenta con un número considerable de empleados, por lo que es de suma importancia establecer pequeñas recomendaciones que pueden servir al momento de reducir amenazas y vulnerabilidades ocasionadas por el recurso humano, como se detalla en la tabla 34.

Tabla 34

Recomendaciones ante vulnerabilidades Humanas.

	Recomendaciones.
Robo de Credenciales.	• Informar al cliente la creación y cambio de las claves de acceso periódicamente. • No facilitar sus credenciales ya que pueden ser utilizadas mediante la web para robo de información afectando la integridad de la institución. • Realizar capacitaciones al personal sobre Ingeniería Social.
Infección de Malware y spam.	• Capacitar al personal de no abrir correos no deseados ya que pueden contener virus, spam o link que puede afectar la integridad de la institución. • Establecer políticas de privilegios o permisos al personal encargado de la administración de los equipos, para evitar su indebido y sin autorización.
Riesgos de Ciberseguridad.	• Emplear procesos automatizados para evitar o eliminar el riesgo del error humano. • Establecer acuerdos de confidencialidad en el personal para protección de información sensible de la institución. • Crear bitácoras manuales o digitales donde se lleve un registro y auditoria de las acciones realizadas por el personal en los activos de la institución.

Nota. La tabla muestra las recomendaciones para vulnerabilidades humanas.

Luego de haber realizado el análisis de los activos identificados en la infraestructura de la institución "Hospital General Alfredo Noboa Montenegro", el cual mediante las pruebas de escaneo se identificó las vulnerabilidades existentes, tratamiento y análisis de riesgos. Con el objetivo de mitigar los riesgos se procedió a tomar acciones correctivas, las cuales se fundamentan en los controles establecidos en el Anexo A de la norma ISO 27001, se procedió aplicar en cada uno de los activos del sistema:

- Políticas de seguridad de la información: es primordial definir reglas para asegurar la protección de la información.

- Seguridad de los recursos humanos: establecer normas y políticas para evitar que los empleados sufran ataques de ingeniería social.
- Gestión de activos: elaborar inventarios de los activos existentes en la infraestructura de red.
- Controles de acceso: crear informes de los accesos a los activos y su administración.
- Gestión de claves: asignar accesos y privilegios a los empleados según su función y el área en la que labora.
- Seguridad física y ambiental: diseño de infraestructura adecuada para seguridad de los activos, para prevención de daños ante desastres naturales.
- Seguridad de las comunicaciones: proponer e implementar equipos de seguridad como firewall, IDP, IPS y cifrado de datos para garantizar la seguridad de la información.
- Mantenimiento del sistema: elaborar un plan de contingencia para la coordinación de mantenimientos periódicos, sean preventivos o correctivos de manera física y lógica para el funcionamiento correcto del sistema.
- Gestión de incidentes de seguridad de la información: crear una base de datos que permita almacenar y administrar los incidentes de acuerdo a su nivel de criticidad.
- Cumplimiento: establecer roles y responsabilidades donde se cumpla con los requisitos, normas y políticas vigentes en el Ecuador en el campo de seguridad informática.

CAPÍTULO V

CONCLUSIONES, RECOMENDACIONES, BIBLIOGRAFÍA, ANEXOS.

5.1.Conclusiones.

- El propósito de la investigación, se inició con un análisis de la situación actual de la institución y elaborar un procedimiento para la gestión de la seguridad informática perimetral de la infraestructura del área de Tecnologías del "Hospital Alfredo Noboa Montenegro", ubicado en la ciudad de Guaranda.

- El procedimiento de evaluación de riesgos en base a la norma ISO/IEC 27001, permitió identificar los riesgos, vulnerabilidades y amenazas en la infraestructura de la institución "Hospital General Alfredo Noboa Montenegro", la utilización e implementación de controles basado en la norma permitió reducir los riesgos de seguridad informática de los activos y proteger la información de la institución.

- El personal del área de Tecnologías de la Información del "Hospital General Alfredo Noboa Montenegro", no conoce detalladamente los lineamientos y uso de la Norma ISO 27001 para el manejo de la seguridad de la información, por tal motivo el siguiente procedimiento para la Gestión de la Seguridad Informática basado en esta norma es la fase inicial para la utilización en la infraestructura de institución y posteriormente para poder obtener una certificación internacional.

- Las herramientas de escaneo como Radip7, NMAP y Nessus, facilito la identificación de vulnerabilidades en los activos con los que cuenta el área de Tecnologías del "Hospital General Alfredo Noboa Montenegro", siendo de gran ayuda conjuntamente con la información compartida del personal de TICS, para la evaluación de riesgos basado en la metodología de MAGERIT en la valoración de sus activos, valoración de amenazas, impacto y evaluación de riesgos.

- Contar con un procedimiento de gestión para le gestión de la seguridad informática en la infraestructura de la institución, estableciendo normas y políticas que en base a cumplir sus lineamientos permita garantizar la integridad, confidencialidad y disponibilidad de la información del "HGANM".

- El procedimiento de seguridad informática perimetral definido en el presente trabajo de titulación, permitirá al personal del área de Tecnologías como guía para actuar antes posibles amenazas que se presenten en la infraestructura de red, evitando su materialización y reduciendo los tiempos de respuesta.

5.2. Recomendaciones.

- Poner en ejecución el Procedimiento de Seguridad informática, el cual sea supervisado por el área de Tecnologías con el propósito de aplicar un plan de mejora a las actividades garantizando la seguridad de la información del "HGANM".

- Es importante concientizar y capacitar a los funcionarios de la institución y proveedores de servicios, sobre el manejo de la información en las instalaciones del "Hospital General Alfredo Noboa Montenegro" y la importancia del objetivo de salvaguardar la información cumpliendo políticas de seguridad y acuerdos de confidencialidad.

- Mantener periódicamente la utilización de herramientas de escaneo para la detección de vulnerabilidades en la infraestructura de la institución, sobre todo cuando se integran nuevos equipos tecnológicos en la red de datos.

- Se recomienda que el departamento de Tecnologías de la Información del "Hospital General Alfredo Noboa Montenegro", se relacione con la norma ISO 27001 y sus controles para llevar una supervisión y funcionamiento eficiente de seguridad de los activos de información.

- La implementación de equipos de seguridad como firewalls, sistema de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS), para proteger los activos de información de la red de datos de la institución.

5.3. Bibliografía.

Bravo, M.J. (2018). Desarrollo De Un Sistema De Gestión De Seguridad De La Información Para Bibliotecas Basado En Una Metodología Mejorada De Análisis De Riesgos Compatible Con La Norma ISO/IEC 27001:2013 Proyecto. https://bibdigital.epn.edu.ec/bitstream/15000/19880/3/CD-9295.pdf

Guacanés, M. (2022). PROPUESTA DE DISEÑO DE UN SGSI BASADO EN LA NORMA ISO/IEC 27001. CASO DE ESTUDIO LA EMPRESA ULTRALINK. http://bibdigital.epn.edu.ec/handle/15000/22812

RODRÍGUEZ, J. (2016). "DISEÑO Y CREACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMATIVA ISO 27000 PARA LA COOPERATIVA CONSTRUCCIÓN, COMERCIO Y PRODUCCIÓN." https://repositorio.uisek.edu.ec/handle/123456789/2013

Alvarado, J. (2020). Análisis De Ataques Cibernéticos Hacia El Ecuador. Revista Científica Aristas, 2(1), 18–27. https://revistacientificaistjba.edu.ec/images/home/documentos/Mayo_2020/2.pdf

Solís, B., Valderrama, H., Tejedor, E., & Vásquez, D. (2023). Seguridad de los Sistemas Informáticos Universitarios: Retos Pendientes. Revista Especializada de Ingeniería y Ciencias de La Tierra, 2(2), 113–142. https://orcid.org/0000-0003-3024-5036

Romero, K. E. (2018). Propuesta de seguridad informática para mejorar el proceso de acceso remoto en una entidad financiera. 132. https://bit.ly/3iO0VmL

ALMEIDA, A. (2022). DISEÑO DE UN PLAN DE SEGURIDAD INFORMATICA PARA MIPYMES. 8.5.2017, 30. https://repository.unimilitar.edu.co/bitstream/handle/10654/43659/AlmeidaDelgadoAlvaroEduardo2O22.pdf.pdf?sequence=1&isAllowed=y

Mendoza, P & Naranjo, D. (2020). Plan de gestión de seguridad de la información para la empresa ALPHA TECHNOLOGIES CIA. LTDA con la norma ISO/IEC 27001:2011. http://bibdigital.epn.edu.ec/handle/15000/20959

Guano, M & Jaramillo, M. (2008). Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio. http://bibdigital.epn.edu.ec/handle/15000/21472

Pilla, C. J. (2019). Diseño De Una Política De Seguridad De La Información Para El Área De Tecnología De La Información De La Cooperativa De Ahorro Y Crédito Chibuleo Ltda., Basado En La Norma ISO/IEC 27002:2013 https://repositorio.uisek.edu.ec/handle/123456789/3601

MINTEL (2020). Guía para la gestión de riesgos y seguridad de información. 31. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GUÍA-PARA-LA-GESTIÓN-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACIÓN-ABRIL-2020.pdf

Vega, E. (2021). LIBRO-SEGURIDAD-INFORMACIÓN.pdf. https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIÓN.pdf

Cuenca, M. P. (2016). Método de gestión de seguridad de la información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001. http://dspace.unl.edu.ec/handle/123456789/11277

Acosta, R. (2022). Propuesta basada en la seguridad lógica perimetral en las pymes, como estrategia para la protección contra ciberataques. https://repository.unad.edu.co/handle/10596/49276

Guerrón, B. (2021). POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL TELETRABAJO EN LA EMPRESA BIOALIMENTAR. In Introducción a la seguridad informática y el análisis de vulnerabilidades. https://repositorio.uta.edu.ec/jspui/handle/123456789/33487

Hidalgo, W. (2023). EVALUACIÓN DE RIESGOS PARA UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LA NORMA ISO/IEC 27001 APLICADO A UN PROVEEDOR DE SERVICIOS DE INTERNET. https://repositorio.uta.edu.ec/jspui/handle/123456789/39448

Cedeño, M. E. (2022). Detección De Vulnerabilidades Mediante Pruebas De Penetración a La Red De Servidores Y Servicios Del Instituto Superior Tecnológico Sucre. Repositorio Universidad Técnica de Ambato. https://repositorio.uta.edu.ec/jspui/handle/123456789/37008

Lucano, L. (2019). Diagnóstico y diseño de un sistema de gestión de seguridad de la información (SGSI), basado en la norma ISO / IEC 27001: 2013, en un banco público. http://www.dspace.uce.edu.ec/handle/25000/18451

Bonilla, M. (2018). Diseño de un sistema de gestión de seguridad de la información bajo la ISO 27000 para la Unidad Educativa Particular Séneca. http://repositorio.uisrael.edu.ec/handle/47000/1748

Lozada, C. (2019). “Estudio de la seguridad informática en el sector de telefonía móvil en Ecuador para la creación de medidas de protección de la información.” https://repositorio.uta.edu.ec/bitstream/123456789/29843/1/Tesis_t1584msi.pdf

AMUTIO, M & CANDAU, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. (Vol. 2006). https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

AMUTIO, M & CANDAU, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II – Catalogo de elementos. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

AMUTIO, M & CANDAU, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III- Guía De Técnicas. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XZojom5FxPY

MINTEL. (2019). Guía de protección de datos-personales MINTEL. 1–13. https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Guía-de-protección-de-datos-personales.pdf

Asamblea Nacional de la República del Ecuador. (2021). Ley Orgánica De Protección De Datos Personales. Registro Oficial Órgano de La República Del Ecuador, 1–70. https://www.salud.gob.ec/wp-content/uploads/2022/09/RO-459-2021-1.pdf

NQA. (2022). Guía de transición ISO 27001:2022. https://www.nqa.com/getmedia/d6e32642-2bc6-4fe8-a7b8-e27054b3083c/Final-27001-Gap-Guide-ES.pdf

5.4.Anexos

ANEXO I

Autorización para desarrollo del Trabajo de Investigación.

UNIVERSIDAD TÉCNICA DE AMBATO
CENTRO DE POSGRADOS
AMBATO – ECUADOR

Guaranda, 8 de mayo del 2023

Hospital Alfredo Noboa Montenegro.
Ciudad de Guaranda

Master.
Franklin Rodrigo Cevallos Molina.
Gerente del HANM
Presente.

De mi consideración:

Yo, **HUGO DAVID PEÑA ROSILLO**, identificado con **C.I 0202048070**, ante Ud. respetuosamente me presento y expongo:

Que actualmente cursando el Maestrado en Tecnología de la Información y Comunicación, mención Seguridad en Redes en la Universidad Técnica de Ambato, solicito a Ud. de la manera más comedida, se considere el permiso y autorización respectiva para realizar el trabajo de Investigación en la Institución sobre **"PROCEDIMIENTO PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA PERIMETRAL EN LA INFRAESTRUCTURA DE UNA ORGANIZACIÓN"** con la finalidad que nos brinde las facilidades de acceso a la **ÁREA DE TECNOLOGÍAS Y COMUNICACIÓN**, con el motivo de recabar información suficiente y necesaria para el desarrollo del proyecto de investigación de acuerdo a la situación actual de la institución.

Gustoso de contar con su ayuda, me permito agradecer su atención a esta solicitud y aprovechar la oportunidad para desearle mis mejores deseos y éxitos en las funciones que usted desempeña.

Saludos cordiales.

Atentamente,

HUGO DAVID PEÑA ROSILLO

Ing. Hugo David Peña Rosillo
C.I. 020204807-0

08-05-2023 15:14

Autorizado
Cevallos
08/05/2023

Ing Raul Coordinar esta actividad.

ANEXO II

FORMATO DE ENTREVISTA APLICADO AL ANALISTA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES.

1. ¿Qué problemas de seguridad informática ha presentado la institución HANM?

……

……

2. ¿Qué problema causo daño perjudicial para la institución y que aún no se pueda controlar en su totalidad?

……

……

3. ¿Para mejorar la eficiencia y calidad de seguridad de la información que ha realizado la institución en conjunto con el departamento de TI?

……

……

4. ¿La institución cuenta con políticas de seguridad para la proteger la información?

……

……

5. ¿Cómo se administrada la red interna del HANM?

……

……

6. ¿Cuál es el estado actual de la seguridad física para acceso a los servidores de la institución?

……

……

ANEXO III

FORMATO DE ENTREVISTA APLICADO AL ANALISTA DE SOPORTE TÉCNICO.

1. ¿Cómo es la administración de software y equipos informáticos para el personal del HANM?

……
……

2. ¿El software utilizado en la infraestructura de la institución cuenta con licencia?

……
……

3. ¿Cuál es el procedimiento de un usuario final para realizar un requerimiento o soporte con el departamento de TI?

……
……

4. ¿Cuál es el proceso para el acceso a la información de los servidores de archivos implementados en la institución?

……
……

5. ¿La organización cuenta con herramientas y estrategias para realizar respaldo de información de cada empleado?

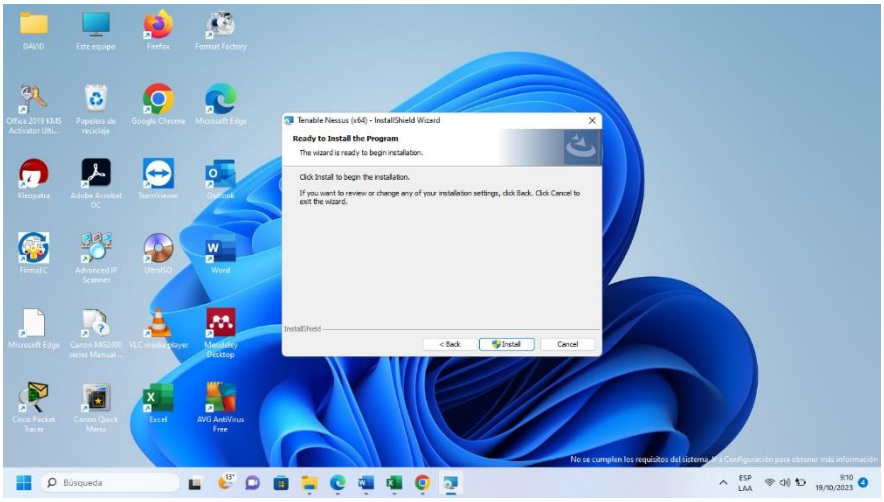
……
……

ANEXO IV

Administración y configuración de software NESSUS.

Figura 34

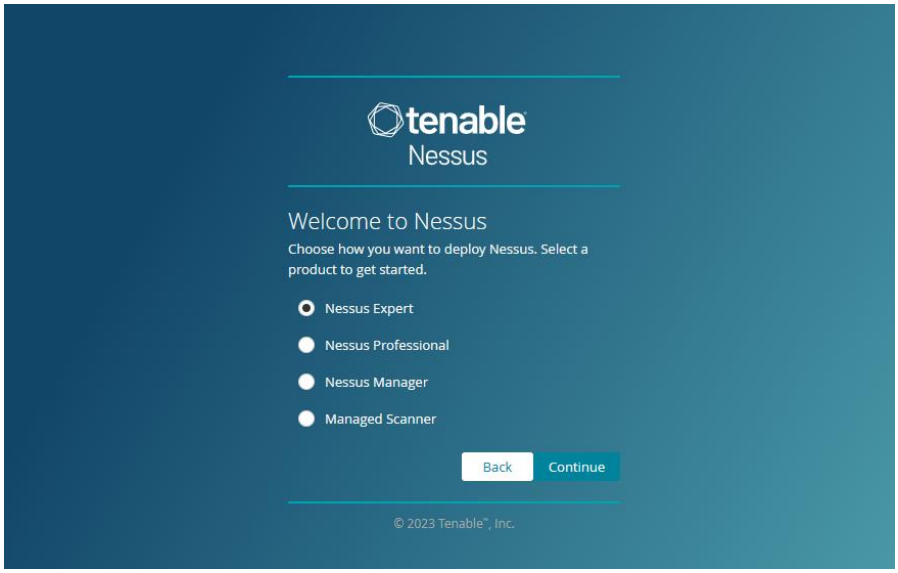
Instalación de aplicación Nessus.



Nota. La figura muestra la descarga e instalación del software.

Figura 35

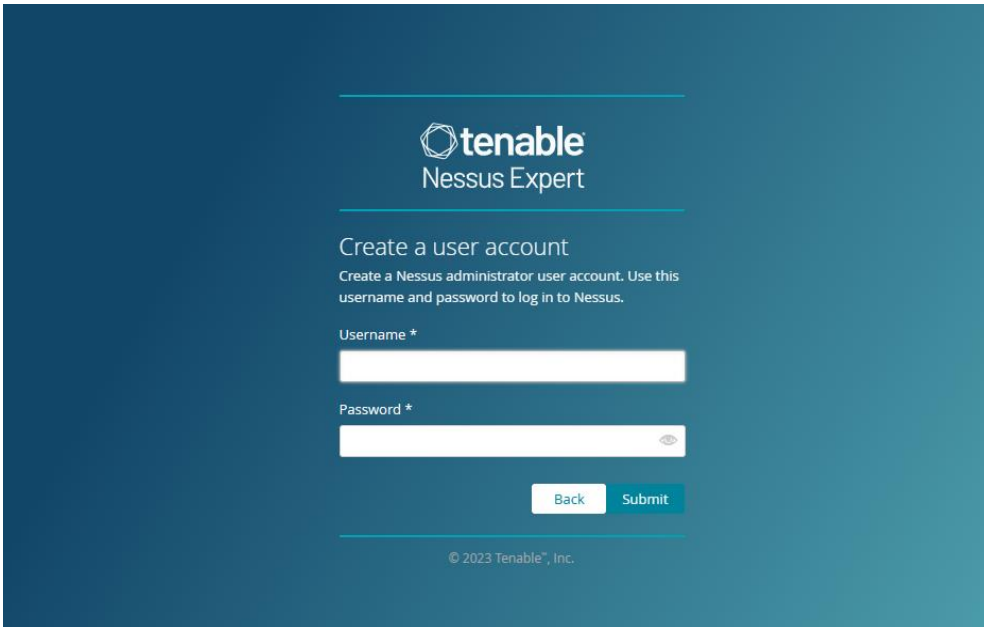
Instalación de aplicación Nessus.



Nota. La figura muestra la interfaz gráfica de Nessus y el tipo de herramienta.

Figura 36

Registro de cuenta Nessus.

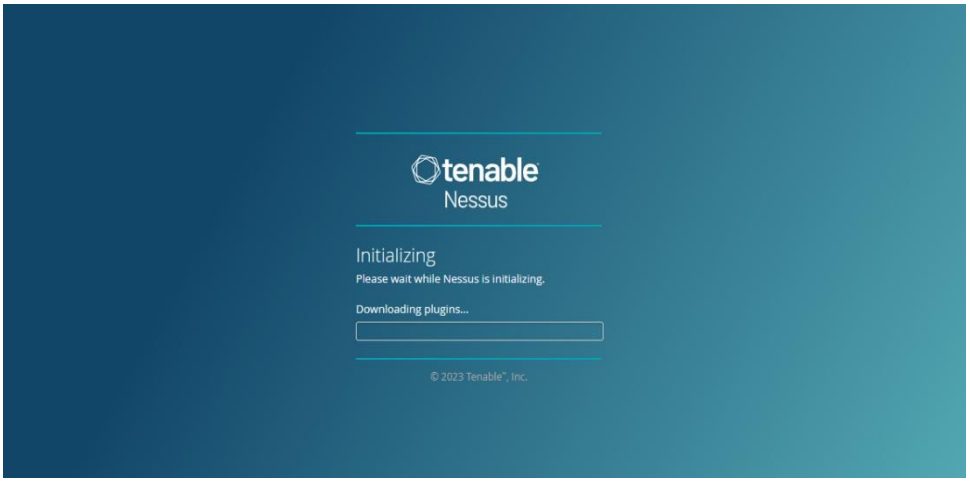


Nota. La figura describe los campos a llenar para el registro de la cuenta.

A continuación, inicia la descarga de los plugin de sus funcionalidades y capacidades del software, como se muestra en la figura 37.

Figura 37

Instalación de complementos y plugin.



Nota. La figura muestra la instalación de sus complementos de la herramienta NESSUS.

En la figura 38, se puede evidenciar que el activo 172.253.144.2 cuenta con una vulnerabilidad de divulgación de información (MITM) debido a un error en la implementación de conjuntos de cifrado que usan AES.

Figura 38

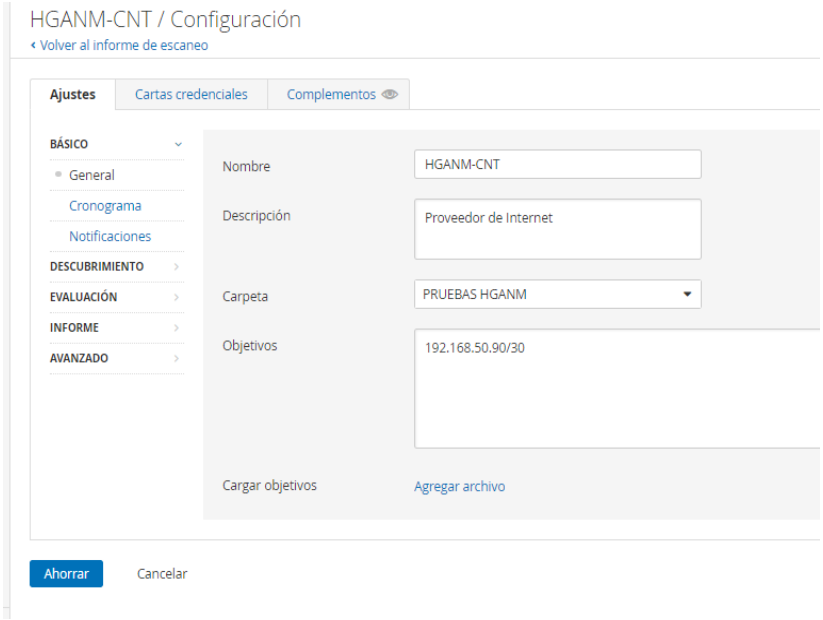
Vulnerabilidad detectada, detalle y solución.

Nota. La figura muestra las posibles remediaciones para la vulnerabilidad detectada.

Se realiza un análisis de escaneo al activo proveedor de internet para lo cual se ingresa el activo 192.168.50.90, como se evidencia en la figura 39.

Figura 39

Ingreso de activo host 192.168.50.90.

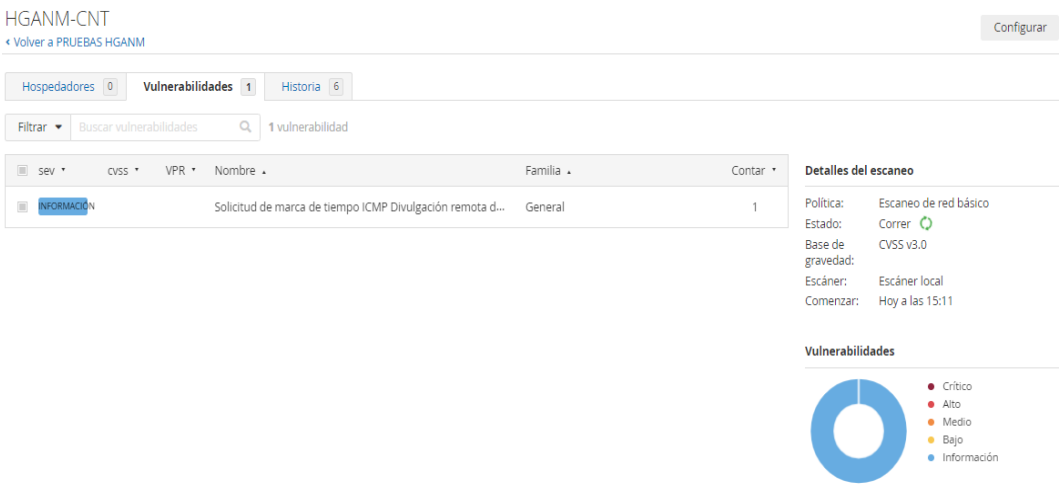


Nota. La figura muestra el ingreso del activo a realizar el análisis.

En el host 192.168.50.90 solo se encuentra vulnerabilidades de datos informativos como se observa en la figura 40.

Figura 40

Vulnerabilidad de datos informativos.

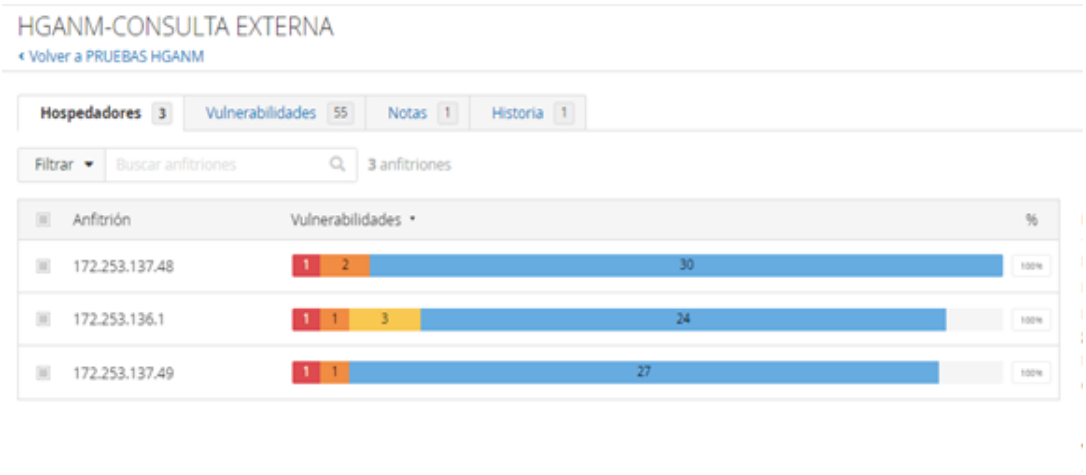


Nota. La figura detalla vulnerabilidades de estado informativo.

En el host 172.253.137.203 se encontró 55 vulnerabilidades entre las categorías critica, alta, medio e informativos, como indica la figura 41.

Figura 41

Vulnerabilidades host 172.253.137.203.



Nota. La figura muestra las vulnerabilidades encontradas en las subredes de cada departamento de la institución.

El software brinda un resumen de las vulnerabilidades identificadas mediante un gráfico expresado en la en donde el 2% de los activos analizados presentan amenazas de nivel alto, el 7% nivel crítico, 25% nivel medio, y el resto son vulnerabilidades de índice bajo o de información, figura 42.

Figura 42

Resumen de vulnerabilidades detectadas.

Nota. La figura muestra de manera general los tipos de vulnerabilidades detectadas en el activo.

Entre las vulnerabilidades de valor critico en el host 172.253.137.203, resalta la no compatibilidad del sistema operativo Unix, como recomendación indica actualización a la versión, se detalla en la figura 43.

Figura 43

Vulnerabilidades host 172.253.137.203

Nota. La figura muestra una solución para el sistema operativo UNIX.

En la figura 44, se evidencia la vulnerabilidad debido a problemas con la actualización del VMware en el host 172.253.137.203.

Figura 44

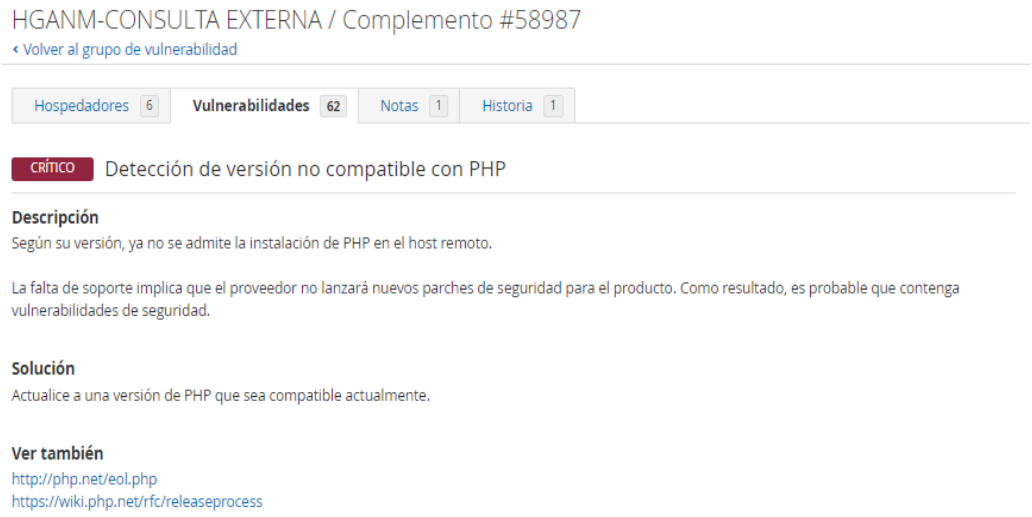
Vulnerabilidad detectada, detalle y solución.

Nota. La figura muestra problemas con la versión de VMware.

El host 172.253.137.203, presenta una vulnerabilidad detectada sobre el PHP no compatible con la versión actual instalada, figura 45.

Figura 45

Vulnerabilidad detectada, detalle y solución.



Nota. *La figura muestra la detección de inconvenientes con el PHP.*

En la figura 46, se detecta una vulnerabilidad de nivel bajo en el host 172.253.137.203.

Figura 46

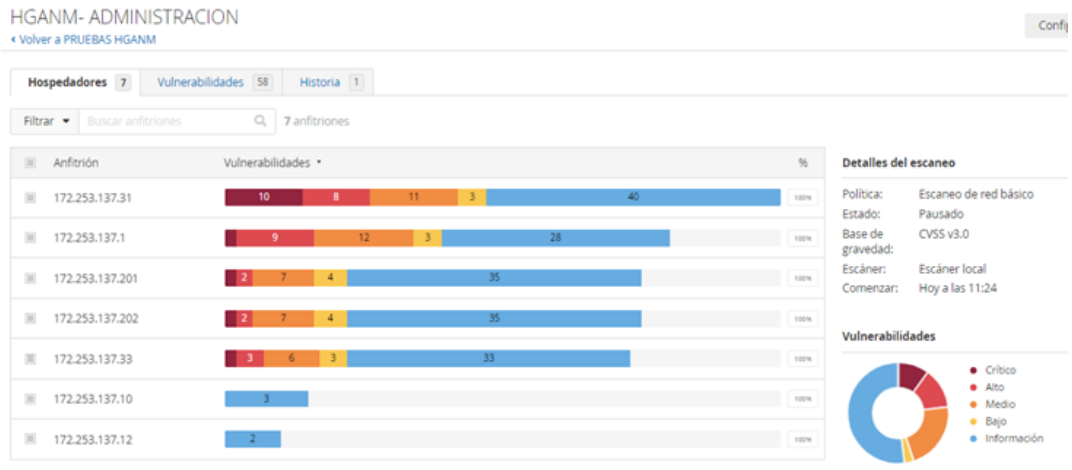
Vulnerabilidad detectada, detalle y solución.

Nota. La figura muestra una vulnerabilidad de nivel bajo detectada en el activo.

Se realiza un escaneo al equipo de conectividad del área administrativa 172.253.137.204 obteniendo los siguientes resultados, evidenciados en la figura 47.

Figura 47

Vulnerabilidades detectadas host 172.253.137.204.

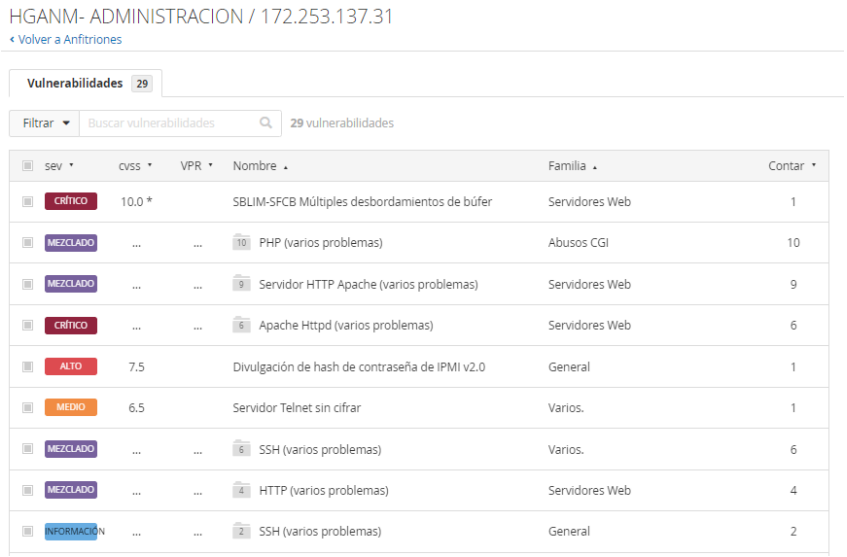


Nota. La figura muestra las vulnerabilidades críticas, altas, bajas y de información.

En la figura 48, se evidencia como vulnerabilidad los desbordamientos del buffer del servidor web, así como problemas con la actualización de la versión del PHP en el host 172.253.137.31.

Figura 48

Vulnerabilidades detectadas host 172.253.137.31.



Nota. La figura muestra las vulnerabilidades detectadas como problemas de HTTP, SSH.

Una vulnerabilidad alta en el host 172.253.137.31, en donde el IPMI se ve afectado por una divulgación de información por problemas de autenticación con el protocolo, detalles figura 49.

Figura 49

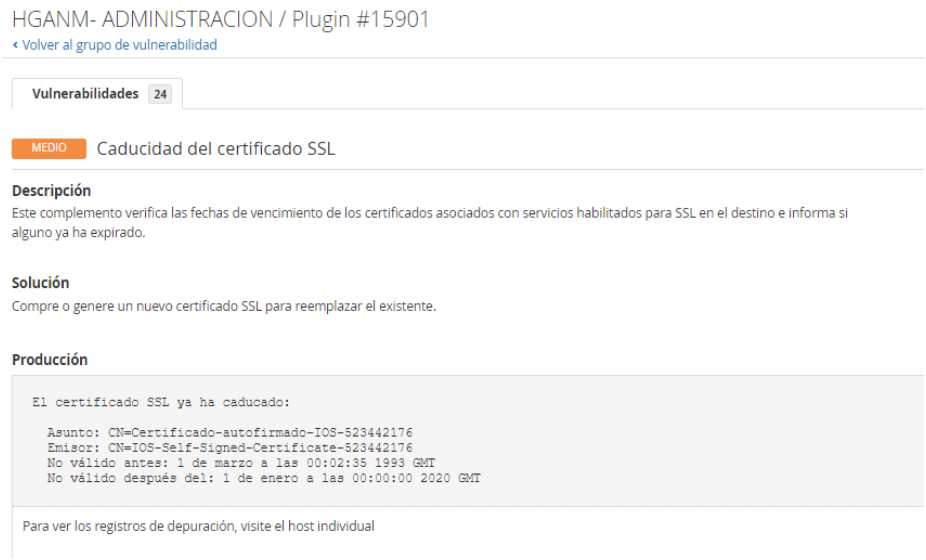
Vulnerabilidad alta, detalles y remediación.

Nota. La figura muestra la solución de deshabilitar el IPMI.

En la figura 50, se puede observar que se detecta la vulnerabilidad del certificado SSL debido a que se encuentra caducado.

Figura 50

Caducidad del certificado SSL, detalles.



Nota. La figura muestra como solución la compra o generación de un nuevo certificado SSL.

También se detecta vulnerabilidad de campo informativo del host 172.253.137.204, como se muestra en la figura 51.

Figura 51

Vulnerabilidades de datos informativos.

Nota. la Figura resalta detección de vulnerabilidades de carácter informativo.

Análisis del host 172.253.137.205, pertenece al área de mantenimiento donde se evidencia todas las redes IP conectadas y sus distintas vulnerabilidades como se evidencia, en la figura 52.

Figura 52

Vulnerabilidades detectadas en el host 172.253.137.205.

Nota. La figura muestra las vulnerabilidades criticas encontradas en los activos.

En el host 172.253.137.120, se detecta 1 vulnerabilidad critica, 5 altas, 10 de nivel medio y 32 de datos informativos como se indica en la figura 53.

Figura 53

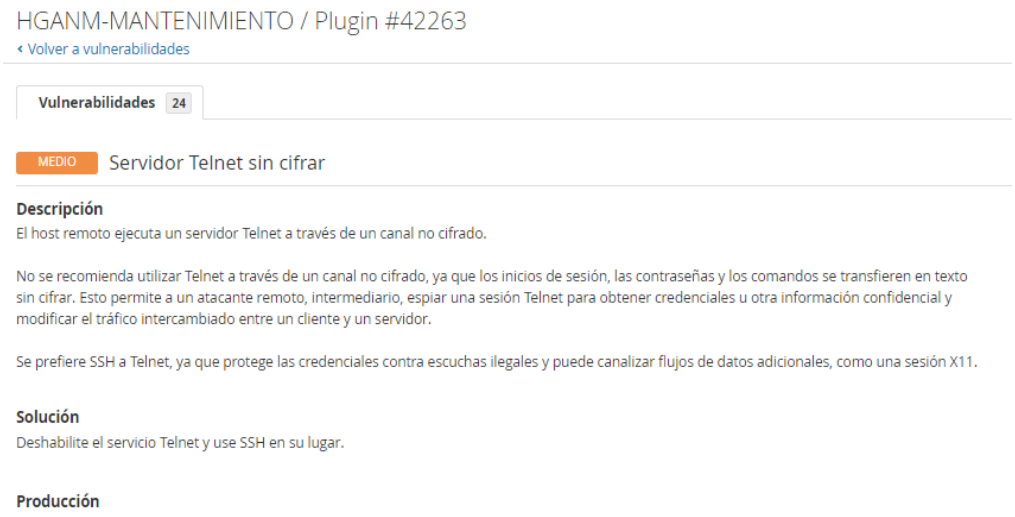
Vulnerabilidades detectadas en el host 172.253.137.210.

Nota. La figura muestra las vulnerabilidades detectadas en el activo del departamento de mantenimiento.

En la figura 54, la vulnerabilidad de nivel medio detectada en relación al servidor telnet, nos recomienda su rehabilitación en el host 172.253.137.205.

Figura 54

Solución deshabilitar el protocolo Telnet.



Nota. La figura resalta como recomendación de no utilizar telnet un canal no cifrado.

La red IP 172.253.137.34, mediante su análisis detecta las siguientes vulnerabilidades como se muestra en la figura 55.

Figura 55

Detección de vulnerabilidades host 172.253.137.34.

Nota. La figura muestra que el activo presenta varios problemas de certificado SSL.

En el host 172.253.137.206, se detectan las siguientes vulnerabilidades como muestra la figura 56.

Figura 56

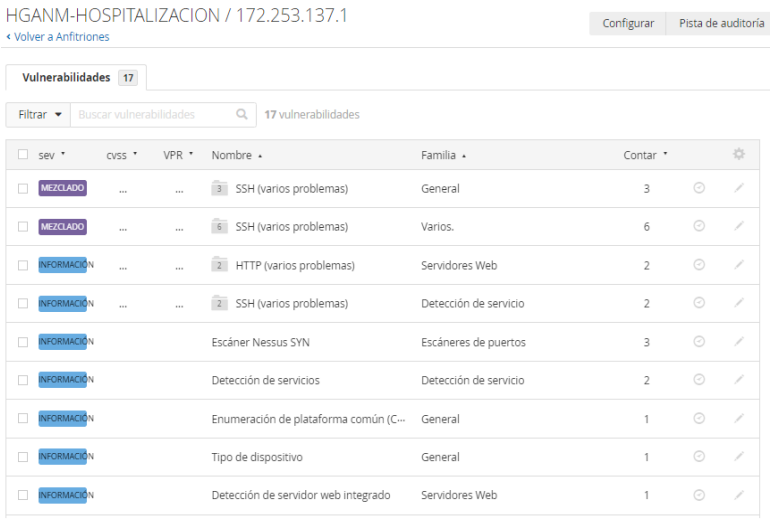
Vulnerabilidades de nivel crítico, alto y medio del host 172.253.137.206.

Nota. La figura resalta la detección de 24 vulnerabilidades de datos informativos.

En el escaneo al host 172.253.137.206, se encontraron 17 vulnerabilidades en la subred 172.253.137.1, como se muestra en la figura 57.

Figura 57

Vulnerabilidades del host 172.253.137.1



Nota. La figura muestra datos informativos de NESSUS.

En el equipo de red interna del departamento de emergencia 172.253.137.208 se encontraron 18 de vulnerabilidades entre las cuales 1 de nivel crítico, medio y 3 de bajo, como se observa en la figura 58.

Figura 58

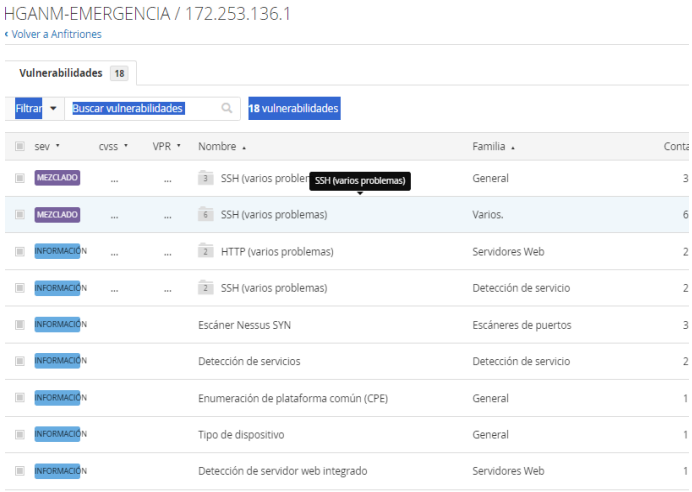
Vulnerabilidades del host 172.253.136.1 – 172.253.137.1

Nota. La figura se puede observar una vulnerabilidad critica.

En el host 172.253.136.1, se puede evidenciar que existe problemas con la actualización del certificado SSH y un dato informativo del servidor web en base al protocolo HTTP, figura 59.

Figura 59

Resultados de escaneo host 172.253.136.1.



Nota. La figura se observa vulnerabilidades en el servidor Web.

En la figura 60, se detecta datos informativos en el escaneo del activo 172.253.137.208.

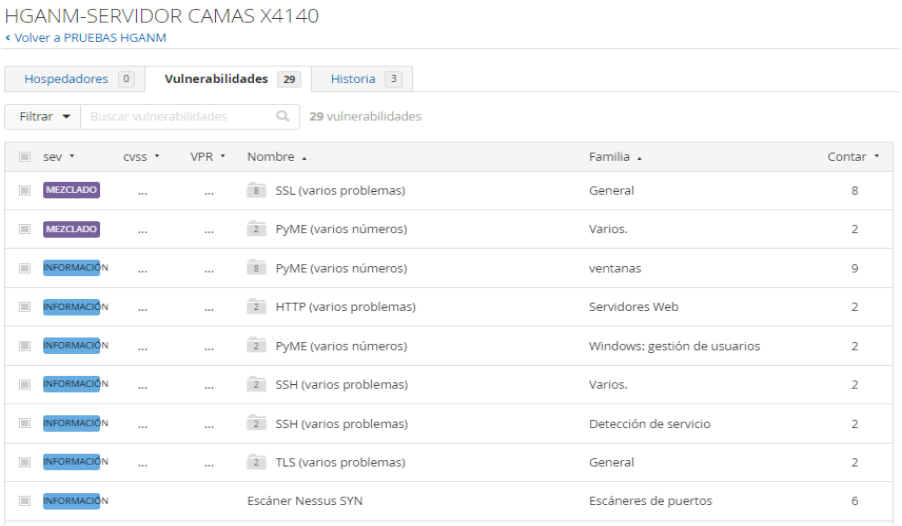
Figura 60

Se detecta 18 vulnerabilidades en el host 172.253.137.208.

Nota. La figura muestra que se debe tomar en cuenta que la vulnerabilidad no causa problemas de seguridad.

Figura 61

Vulnerabilidades host 190.152.181.94.

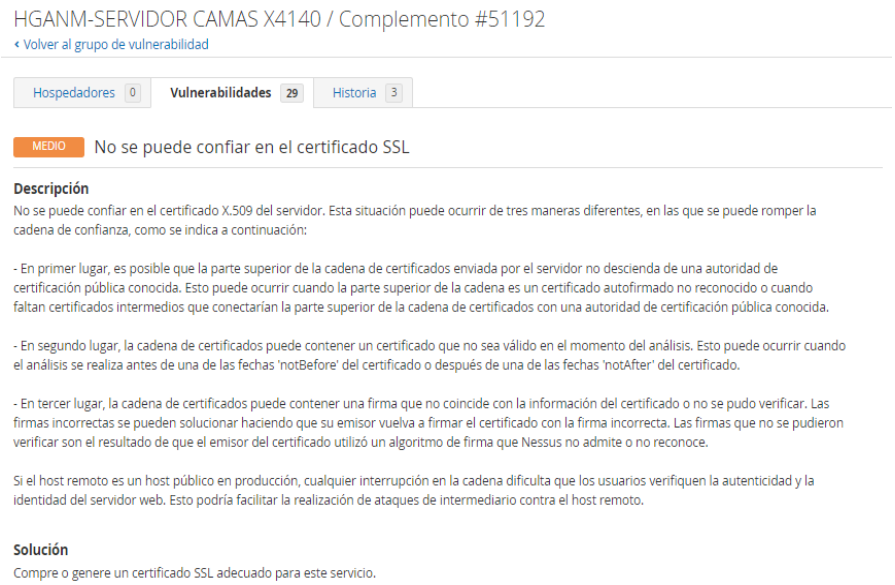


Nota. La figura muestra que se detectó 29 vulnerabilidades.

Para el host 190.152.181.94, se recomienda la compra o la actualización de un certificado SSL adecuado para el servicio ante la vulnerabilidad de nivel medio detectada, detalles en la figura 62.

Figura 62

Posible solución para el host 190.152.181.94.



Nota. La figura muestra que la vulnerabilidad es de tipo bajo relacionada al certificado SSL.

Figura 63

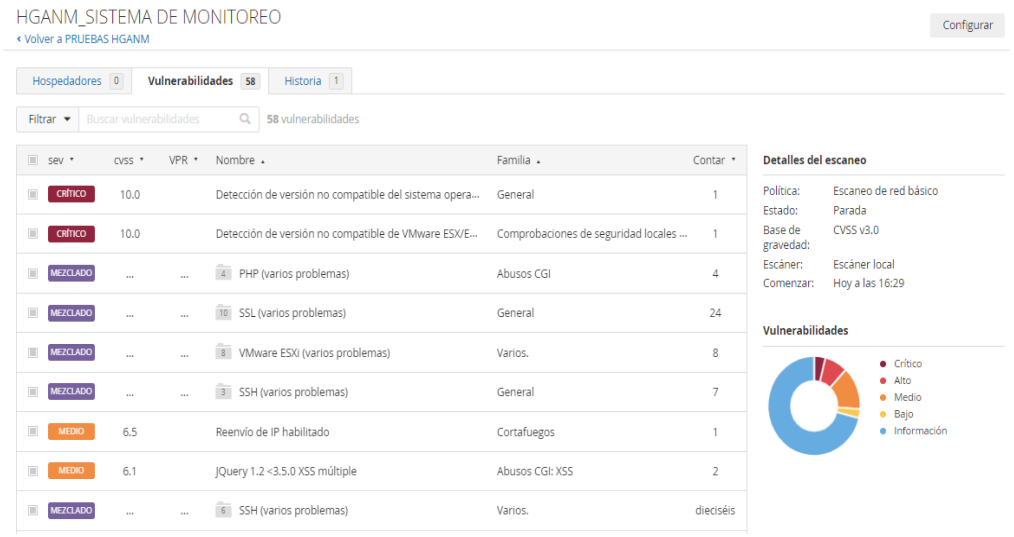
Vulnerabilidades informativas para el host 190.152.181.94.

Nota. La figura muestra la detección de 29 Vulnerabilidades informativas en el servidor de gestión de camas.

El host ACKP cuya funcionalidad es el monitoreo del servidor, durante su escaneo a la IP asignada 172.253.160.46 se evidencia las siguientes vulnerabilidades en la figura 64.

Figura 64

Vulnerabilidades en el host 172.253.160.46



Nota. La figura muestra los tipos de vulnerabilidades detectadas durante el análisis.

El activo 172.253.160.46 presenta un problema critico por la desactualización de su sistema operativo UNIX, figura 65.

Figura 65

Vulnerabilidad critica en el host 172.253.160.46.

Nota. La figura resalta la solución de actualizar el sistema operativo Unix.

Figura 66

Vulnerabilidad critica en el host 172.253.160.46.

Nota. La figura muestra que se tiene fallas con la versión del PHP.

En la figura 67, se puede evidenciar una vulnerabilidad de carácter medio y su posible remedición como solución en el host 172.253.160.46.

Figura 67

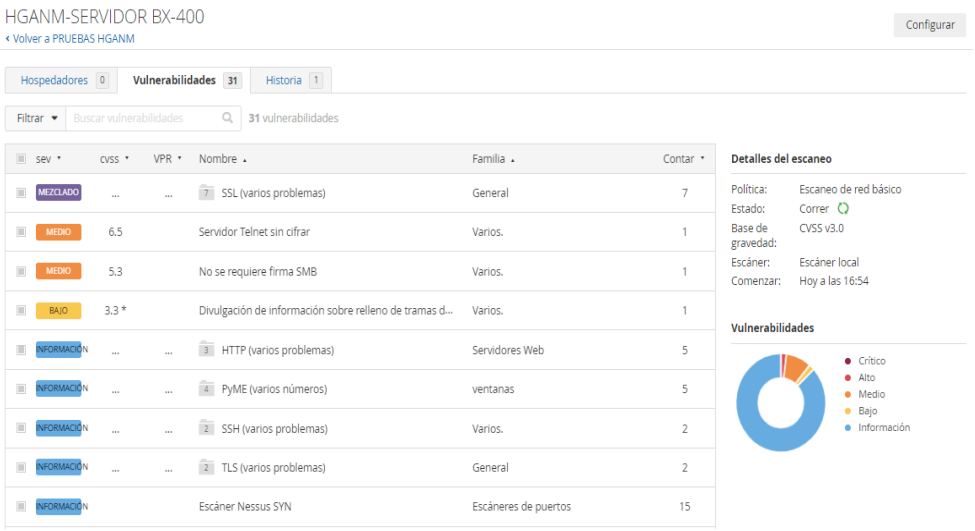
Vulnerabilidad detectada en el host 172.253.160.46.

Nota. La figura se puede observar que el sistema de monitoreo cuenta con una vulnerabilidad de reenvió de IP.

Mediante el escaneo realizado al servidor de la página web de la institución 172.253.160.13, se encontró las siguientes debilidades como se muestra en la figura 68.

Figura 68

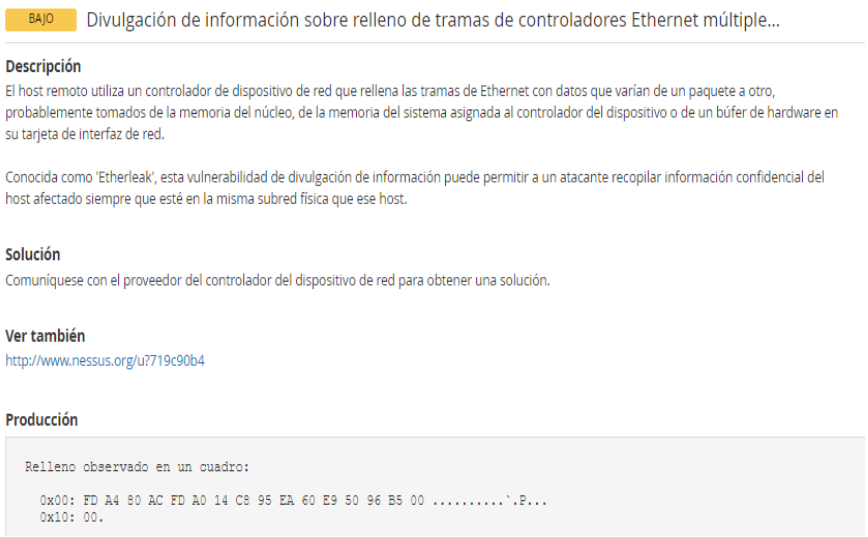
Vulnerabilidad en el host 172.253.160.13



Nota. la figura muestra vulnerabilidades de tipo medio en el servidor Telnet.

Figura 69

Vulnerabilidad de nivel bajo y su solución.



Nota. La figura muestra que el dispositivo utiliza un controlador envía tramas a nivel ethernet.

En el servidor 172.253.160.13 también se evidencia vulnerabilidades en lo que se refiere a datos informativos, ver figura 70.

Figura 70

Vulnerabilidad del servidor 172.253.160.13.

Nota. La figura muestra que se encuentra vulnerabilidades informativas en servidor de gestión de camas hospitalaria.

ANEXO V

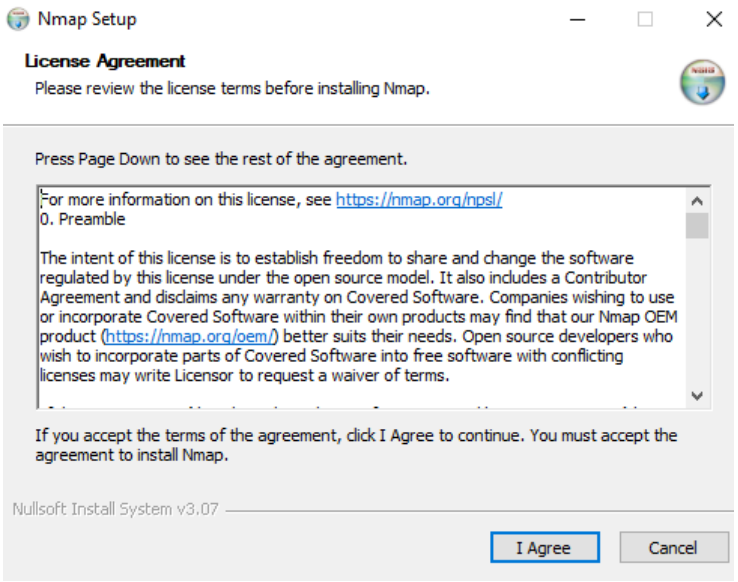
Administración y configuración de la herramienta NMAP.

Primer paso. Descargar el archivo de instalación.

Ejecutamos el programa como administrador y procedemos con la instalación, como se muestra en la figura 71.

Figura 71

Pasos de instalación de software NMAP.



Nota. La figura muestra los pasos de instalación de NMAP.

Figura 72

Pasos de instalación de software NMAP.

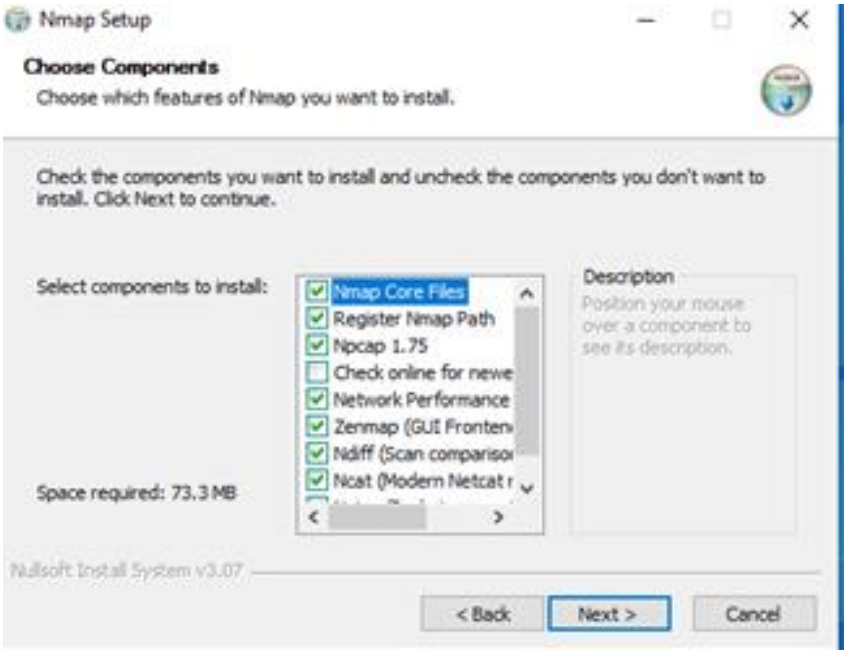
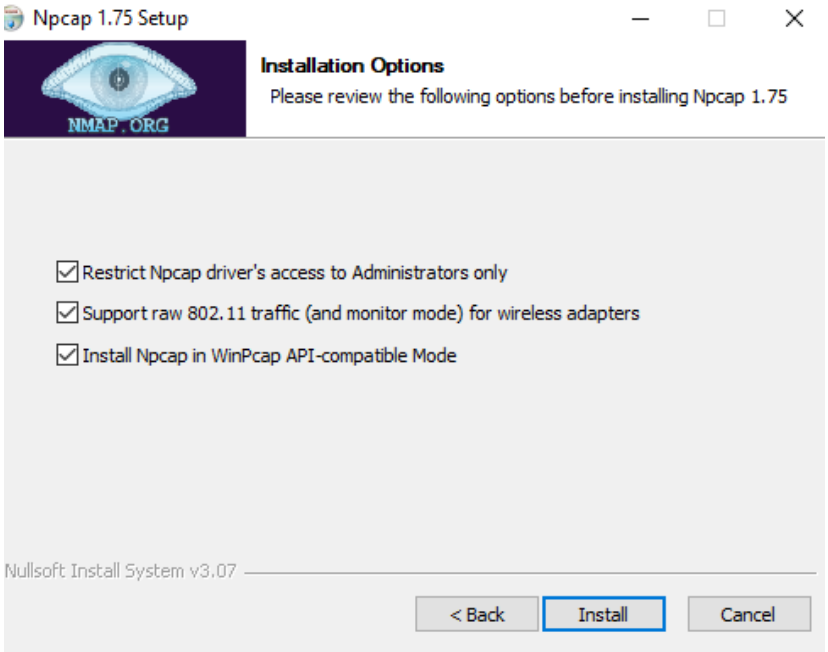


Figura 73

Finalización de instalación de software NMAP.

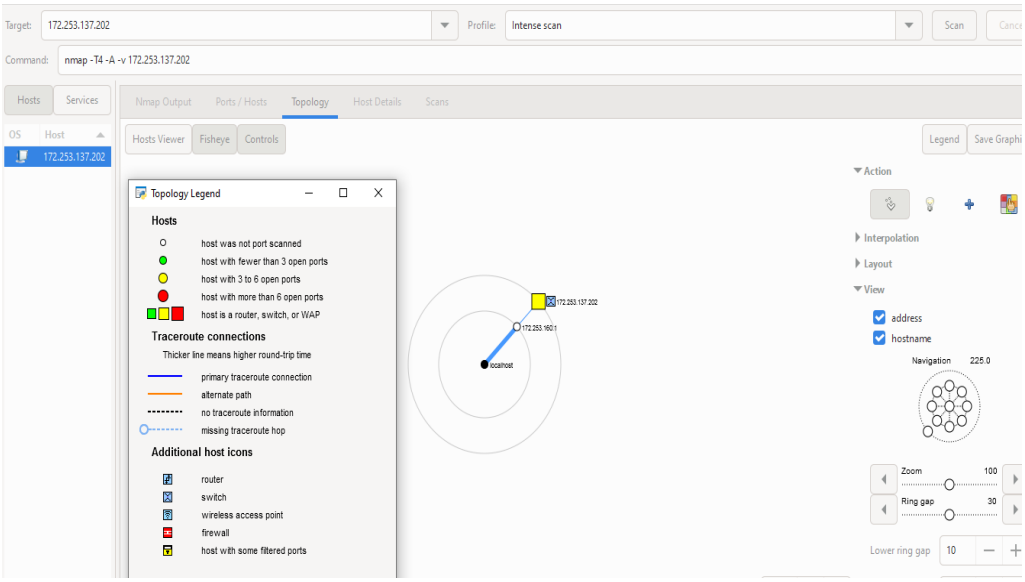


Nota. La figura muestra los pasos de instalación de NMAP.

NMAP permite visualizar de forma gráfica la ubicación del activo, dentro del diseño de la topología de red de la institución, figura 74.

Figura 74

Diseño de red activo 172.253.137.202.



Nota. En la figura se puede observar el diseño de red cada que se ingresa un activo.

En la figura 75, mediante el escaneo a la red 172.253.144.2 se muestra que el puerto 21 utilizado para transferencia de archivos se encuentra cerrado dentro del equipo que cumple de firewall en la institución.

Figura 75

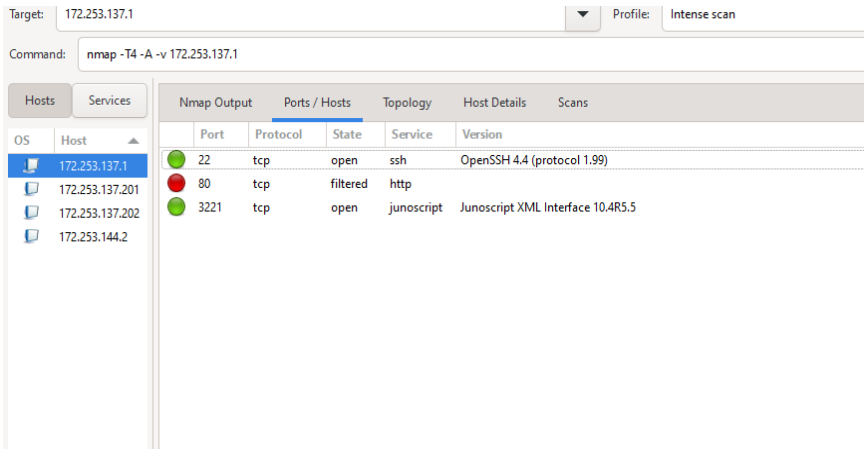
Puertos cerrados en la red 172.253.144.2.

Nota. La figura muestra que NMAP permite evaluar el estado de los puertos de conexión.

El activo de la institución con la IP asignada 172.253.137.1, mediante su análisis se evidencia el estado de sus puertos como se observa en la figura 76.

Figura 76

Puerto para servidores web (80) cerrado.

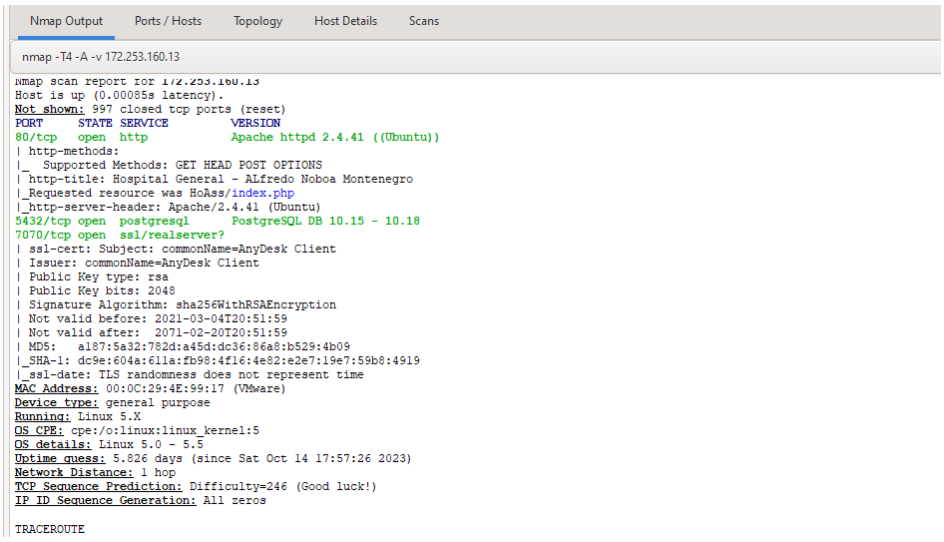


Nota. La figura muestra el estado de los puertos disponibles en el activo.

En la IP 172.253.160.13 asignada al servidor de la página web, se puede verificar el puerto abierto de la aplicación SQL y su versión apache, figura 77.

Figura 77

Análisis servidor web 172.253.160.13

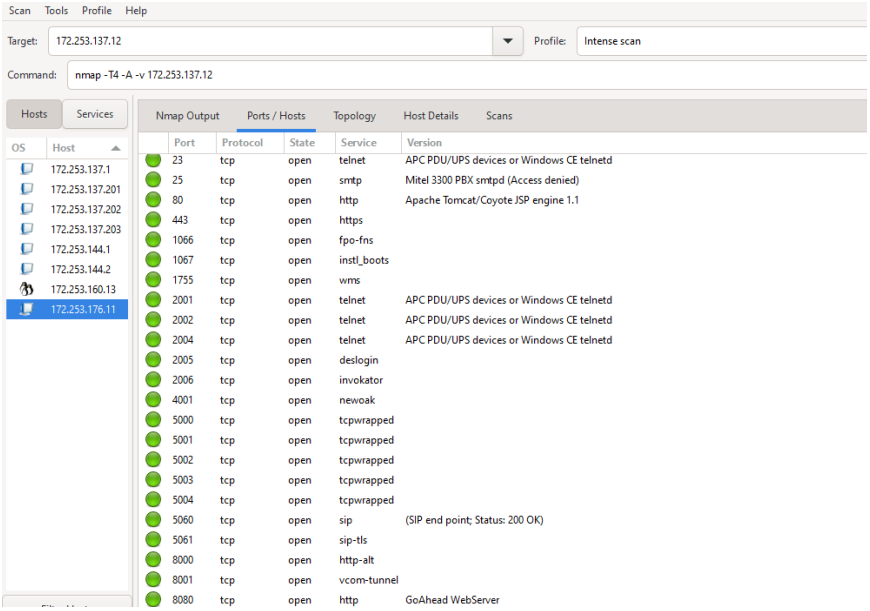


Nota. La figura detalla los datos informativos del activo, sistema operativo, MAC Address, etc.

En la figura 78, se puede verificar los puertos disponibles en el equipo MITEL (controlador VOIP) con la IP asignada 172.253.137.12.

Figura 78

Puertos disponibles controlador VOIP.

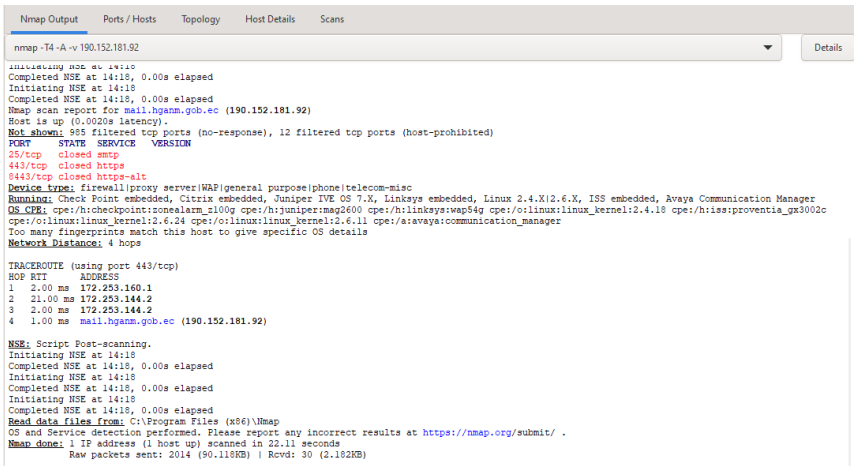


Nota. La figura muestra los puertos disponibles en la central telefónica MITEL.

Finalmente se escaneo el host 190.152.181.92, como resultado tenemos 3 puertos cerrados, como se puede ver en la figura 79.

Figura 79

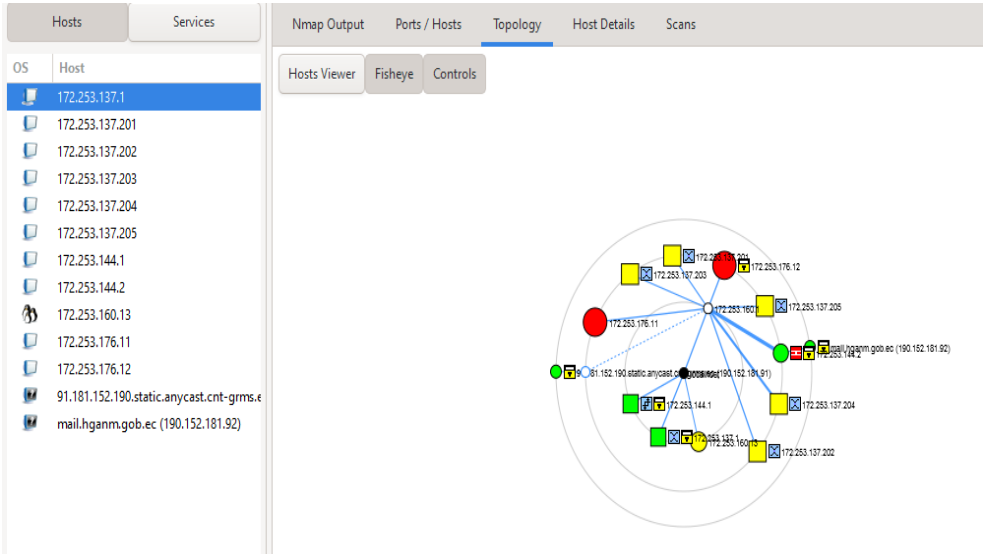
Puertos cerrados SMNTP, HTTPS y HTTPS-ALT.



Nota. La figura muestra puertos asignados para los protocolos de comunicación.

Figura 80

Hosts existentes en la topología de red del HGANM.



Nota. La figura muestra diseño de la infraestructura de red de los hosts existentes en la institución "Hospital Alfredo Noboa Montenegro".

ANEXO VI

Instalación de software y pruebas de análisis con Rapid7.

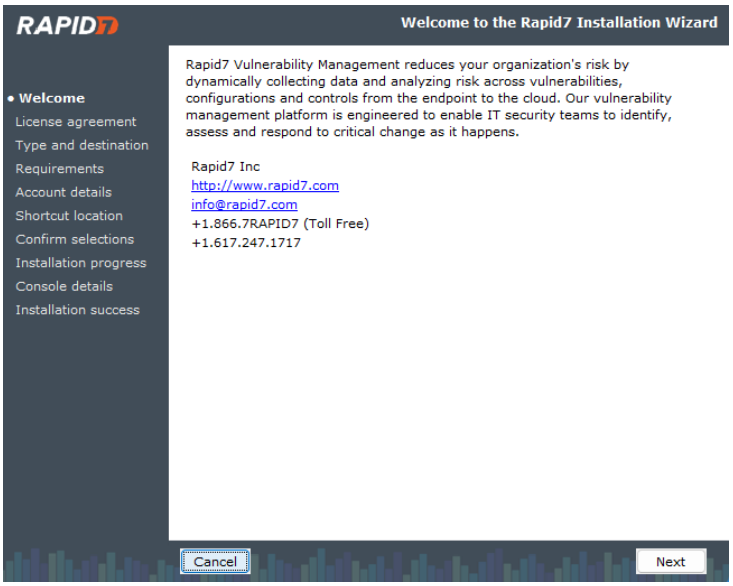
Figura 81

Registro de cuenta para descarga de software.

Nota. La figura muestra los pasos para el registro y activación de cuenta.

Figura 82

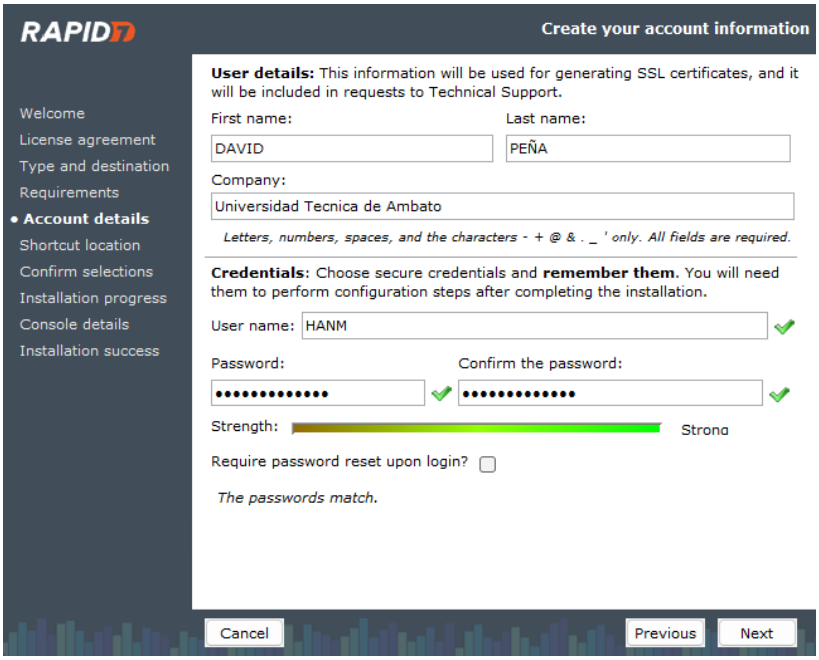
Instalación de software Rapid7.



Nota. La figura muestra los pasos para la instalación de Rapid7.

Figura 83

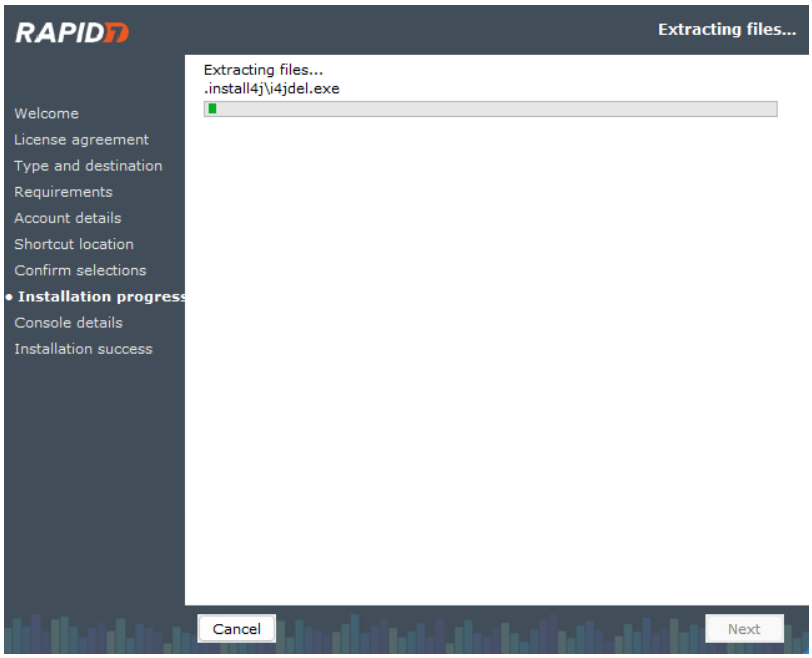
Registro y confirmación de la cuenta.



Nota. La figura muestra los campos para confirmación de la cuenta.

Figura 84

Progreso de la Instalación.

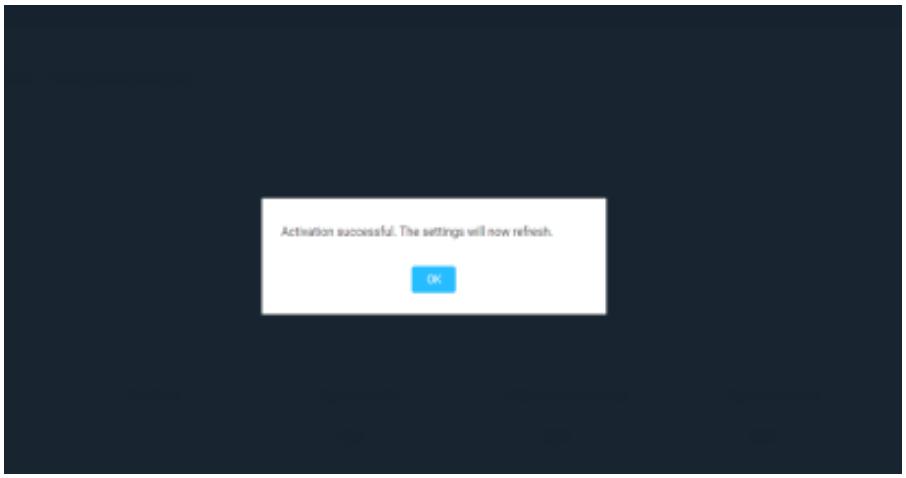


Nota: La figura muestra la instalación del software Rapid7.

Se procede activar la cuenta con el código de autenticación que llega al correo electrónico una vez registrado en la página de nexpose, como se muestra en la figura 85.

Figura 85

Activación completa de la cuenta.

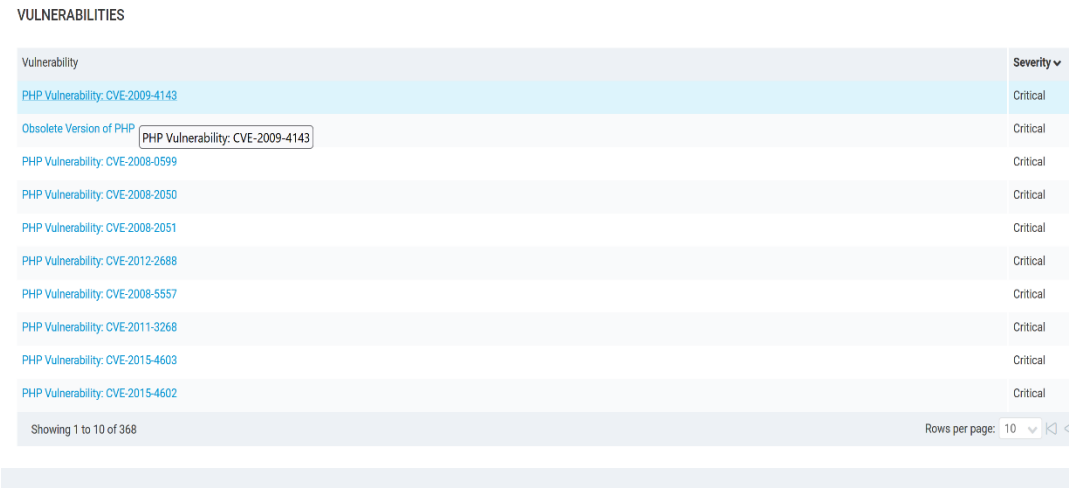


Nota. La figura muestra la activación de la cuenta con la clave generada en NEXPOSE.

Se repite el proceso para realizar el escaneo a todos los activos existentes en la infraestructura del "Hospital General Alfredo Noboa Montenegro", figura 86.

Figura 86

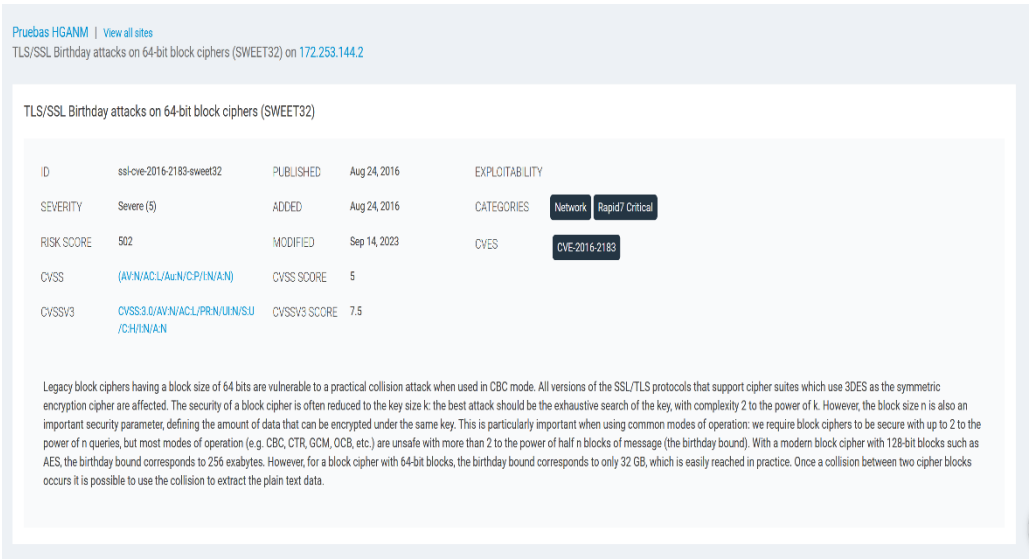
Vulnerabilidad de PHP en el host 172.253.144.



Nota. La figura muestra las vulnerabilidades relacionadas al PHP encontradas en el activo.

Figura 87

Vulnerabilidad de protocolo TSL/SSL en el host 172.253.144.2.

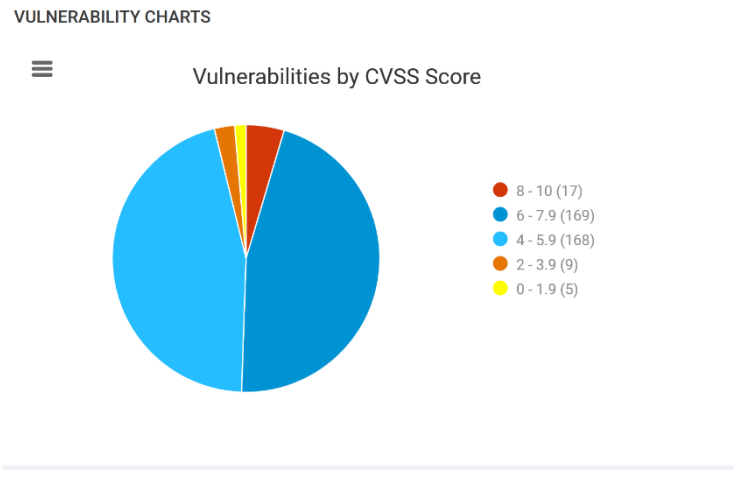


Nota. La figura detalla vulnerabilidad con problemas con el protocolo SSL/TLS en el servidor.

La herramienta también detalla los resultados obtenidos del host 172.253.144.2, de forma estadística grafica de las vulnerabilidades detectadas, figura 88.

Figura 88

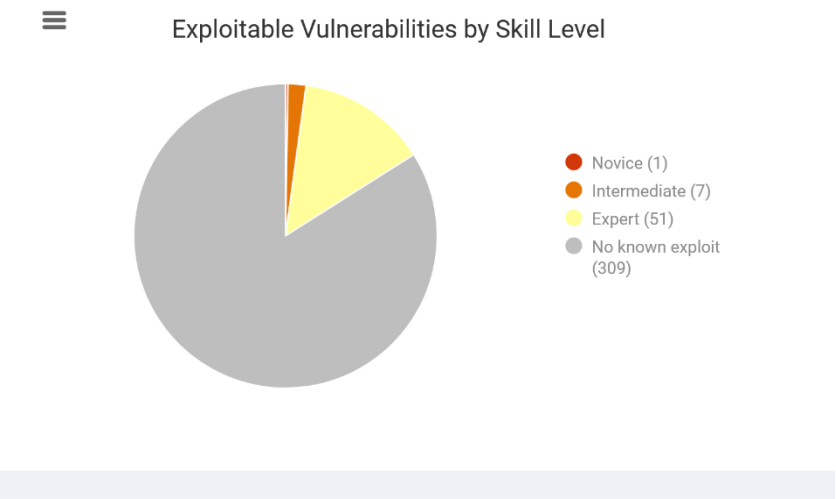
Vulnerabilidad del host 172.253.144.2.



Nota. La figura muestra las vulnerabilidades por nivel de criticidad.

Figura 89

Vulnerabilidad por nivel de habilidad del host 172.253.144.2.

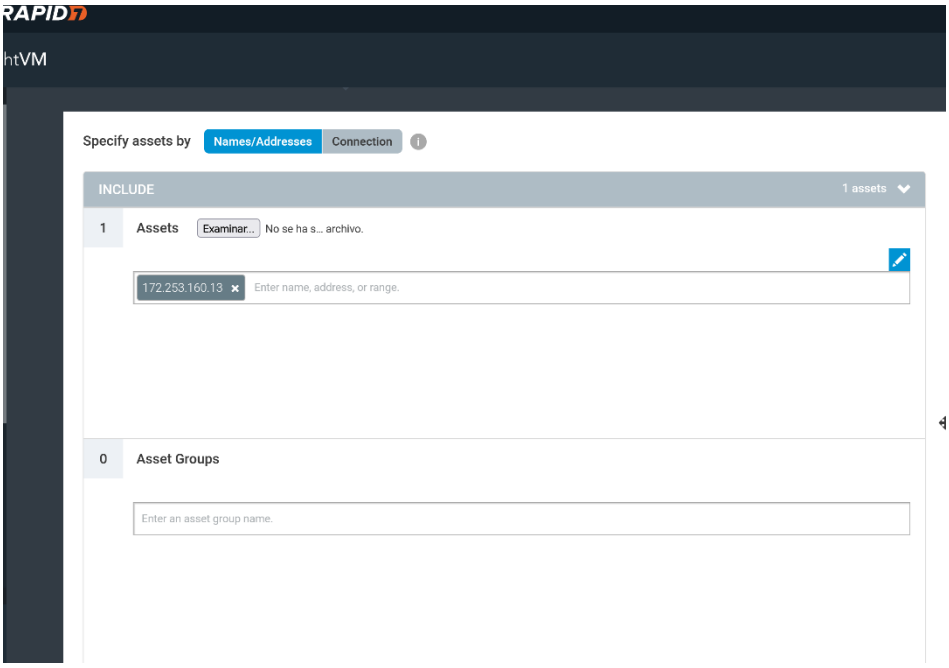


Nota. La figura muestra las vulnerabilidades por nivel de criticidad.

Se crea un sitio para el análisis de detección de vulnerabilidades del servidor de la página web – hoste 172.253.160.13, como se observa en figura 90.

Figura 90

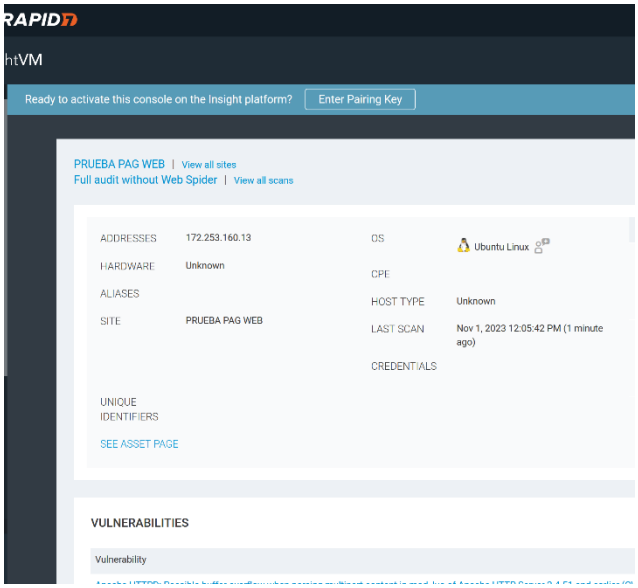
Análisis de vulnerabilidades del servidor 172.253.160.13.



Nota. La figura muestra la creación del sitio para el análisis del servidor web.

Figura 91

Sistema operativo del servidor 172.253.160.13.

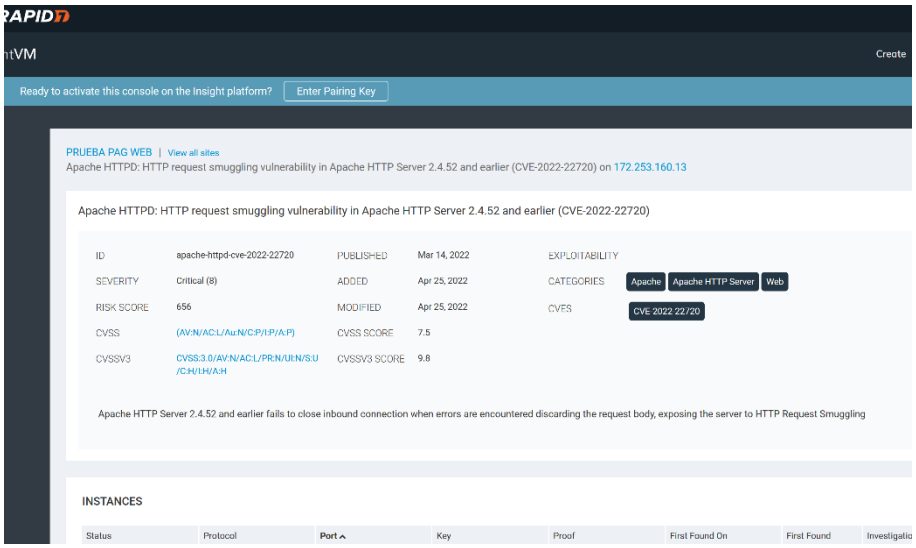


Nota. La figura muestra las características del sistema operativo del servidor web.

En el host 172.253.160.13, del servidor de la página web se detecta vulnerabilidades con el servidor Apache HTTP, como se observa en la figura 92.

Figura 92

Vulnerabilidad con el servidor Apache HTTP / 172.253.160.13.

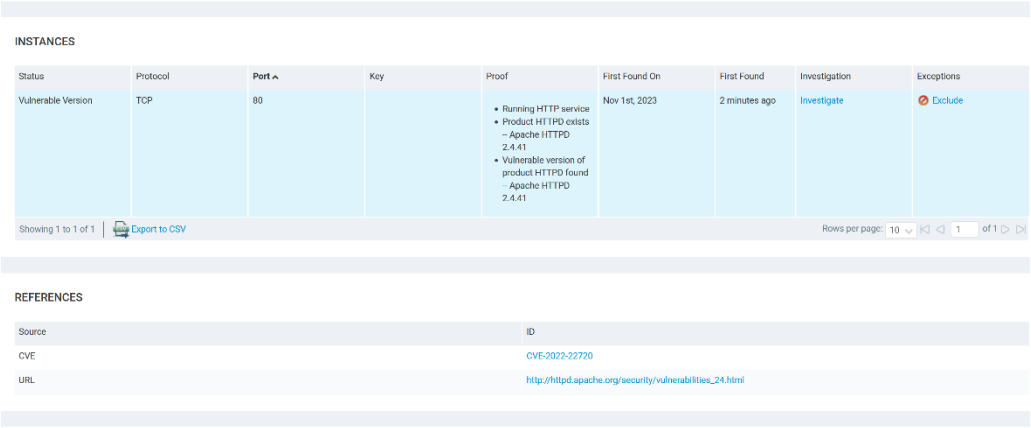


Nota. La figura muestra una vulnerabilidad critica en el servidor Apache HTTP.

En la figura 93, podemos observar de una manera más detallada la vulnerabilidad del protocolo Apache HTTPD, puerto de conexión del host 172.253.160.13.

Figura 93

Especificaciones vulnerabilidad protocolo Apache HTTPD.

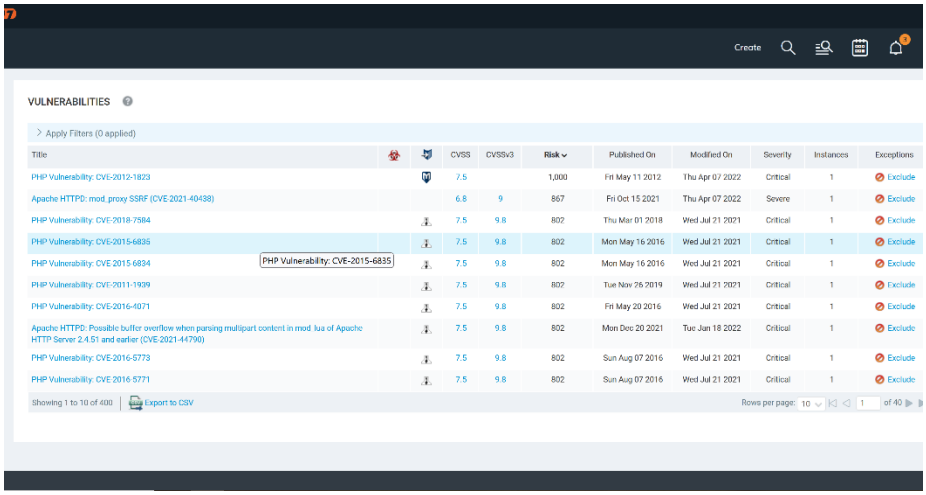


Nota. La figura muestra las instancias y posibles soluciones de las vulnerabilidades.

En la siguiente prueba de escaneo se puede verificar las vulnerabilidades existentes referidas a PHP, Apache, etc. del host 172.253.160.13, figura 94.

Figura 94

Vulnerabilidades existentes en el host 172.253.160.13.

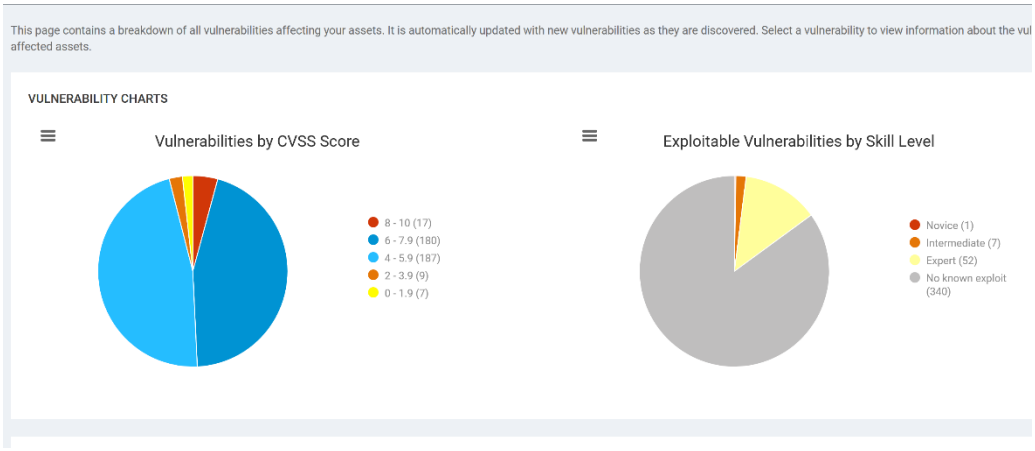


Nota. La figura detalla todas las vulnerabilidades relacionadas el PHP.

En la figura 95, tenemos una representación gráfica de las vulnerabilidades clasificadas por niveles critica, alta, media en el escaneo realizado al host 172.253.160.13.

Figura 95

Clasificación de vulnerabilidades por niveles.

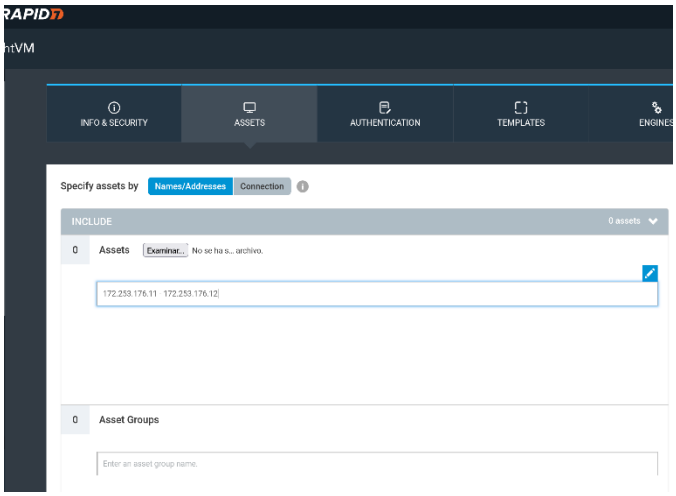


Nota. La figura muestra la representación gráfica de las vulnerabilidades por clasificación de criticidad**.**

Se procede a realizar el escaneo de los activos de servicio de VoIP de los siguientes hosts 172.253.176.11 – 172.253.176.12, figura 96.

Figura 96

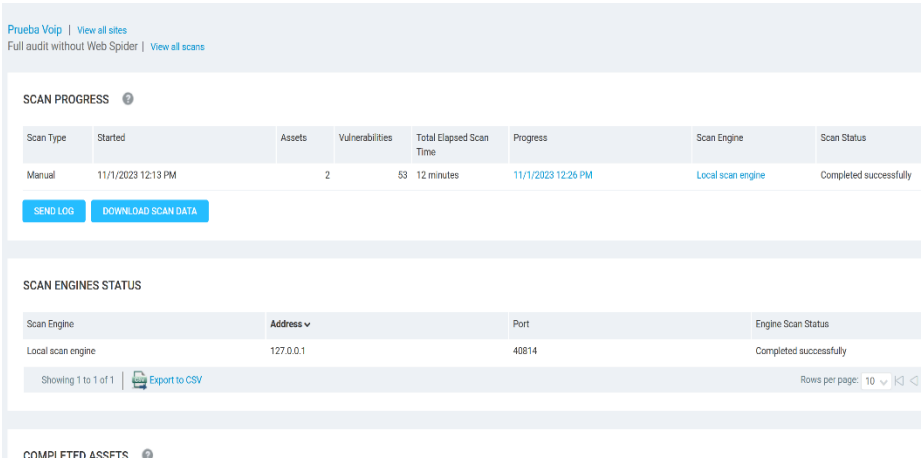
Configuración del sitio para escaneo de activos de VoIP.



Nota. La figura muestra el ingreso de los activos de VOIP en el sitio creado.

Figura 97

Detección de vulnerabilidades activos de VoIP.

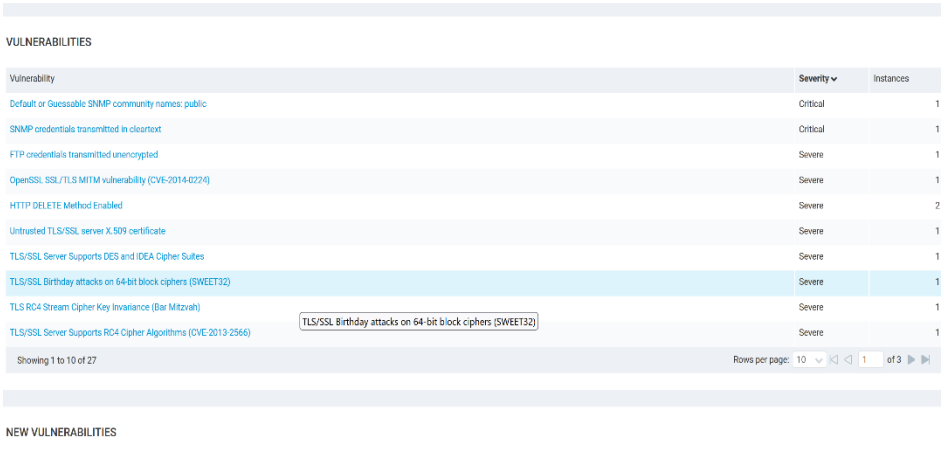


Nota. La figura muestra que se encontraron 57 vulnerabilidades en servicio de VOIP.

En la figura 98, se detecta vulnerabilidades relacionados a protocolos SNMP, FTP, OpenSSL, etc. En los hosts 172.253.176.11 – 172.253.176.12.

Figura 98

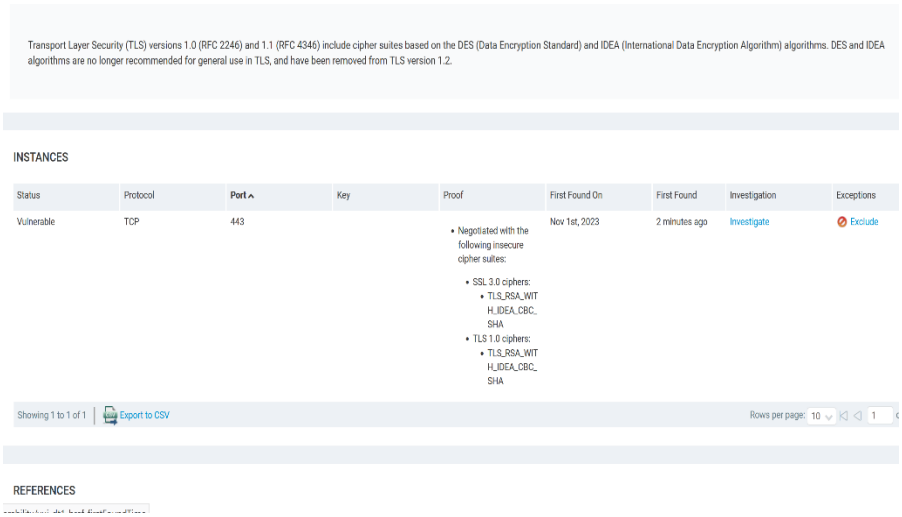
Vulnerabilidades hosts 172.253.176.11 – 172.253.176.12.



Nota. La figura se puede observar las vulnerabilidades críticas en el protocolo SNMP.

Figura 99

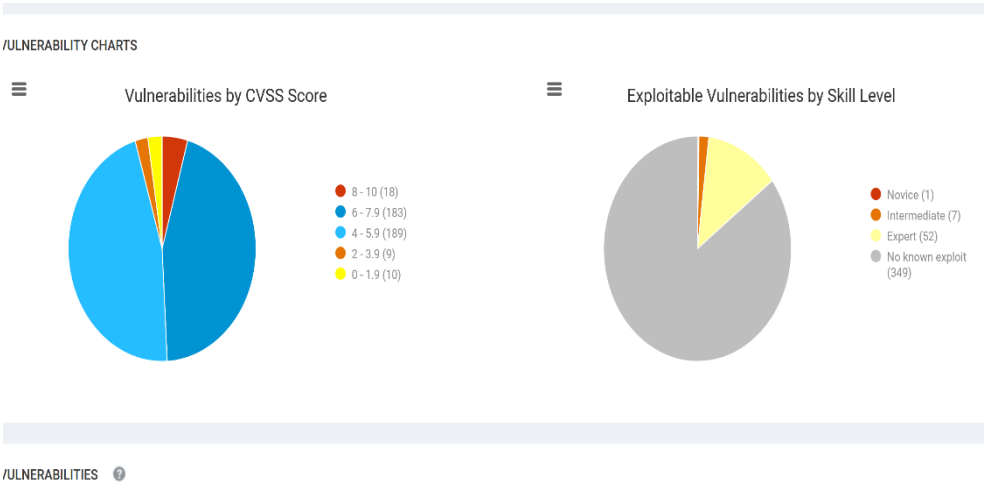
Vulnerabilidad TRANSPORT LAYER SECURITY.



Nota. La figura muestra evidenciar las instancias de la vulnerabilidad presente relacionada con TRANSPORT LAYER SECURITY (TLS).

Figura 100

Vulnerabilidad activos 172.253.176.11 – 172.253.176.12.

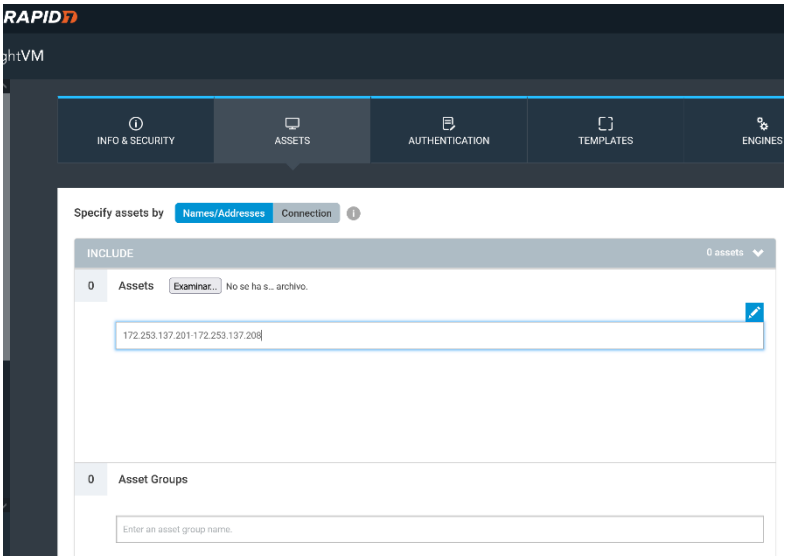


Nota. La figura muestra Interpretación gráfica de las vulnerabilidades existentes en los activos

Escaneo de la red interna compuesta por los distintos departamentos de la institución a cada switch 2960, mediante el ingreso de los activos en el rango de 172.253.137.201 – 172.253.137.208, como se observa en la figura 101.

Figura 101

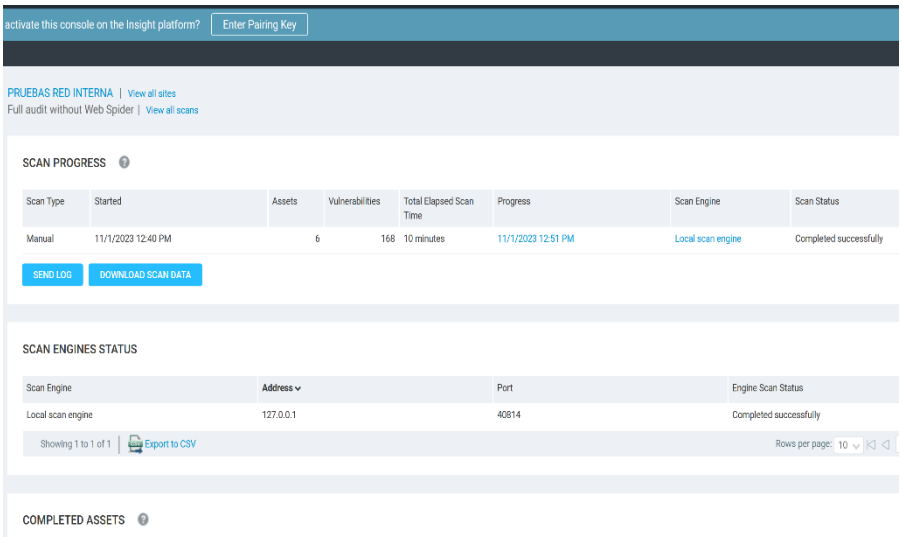
Creación del sitio de escaneo de nuevos activos.



Nota. La figura muestra el ingreso de los activos de la red interna de la institución.

Figura 102

Detección de 168 vulnerabilidades.

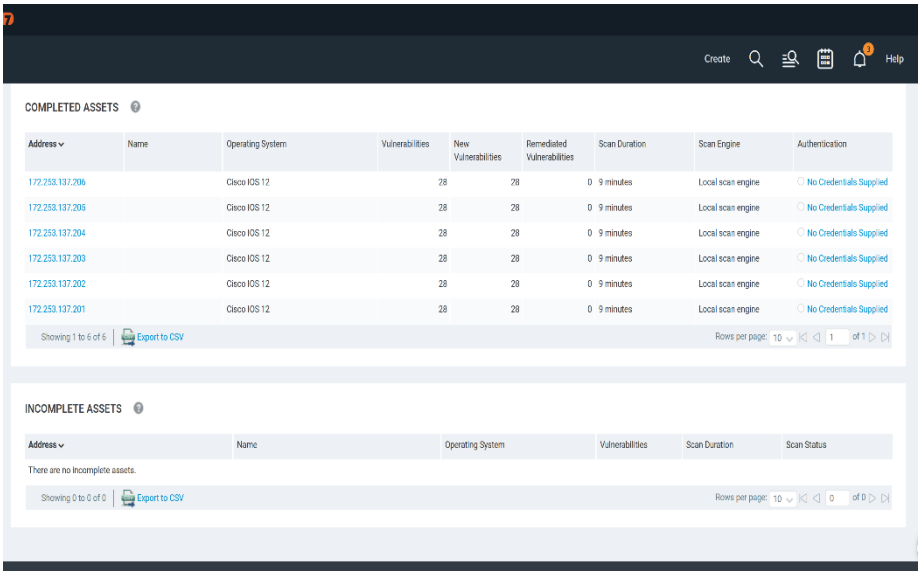


Nota. La figura muestra el análisis a la red interna de la institución.

En la figura 103, se registra una tabla detallada de los activos que componen la red interna de la institución con su número total de vulnerabilidades detectadas.

Figura 103

Información de vulnerabilidades por activo.

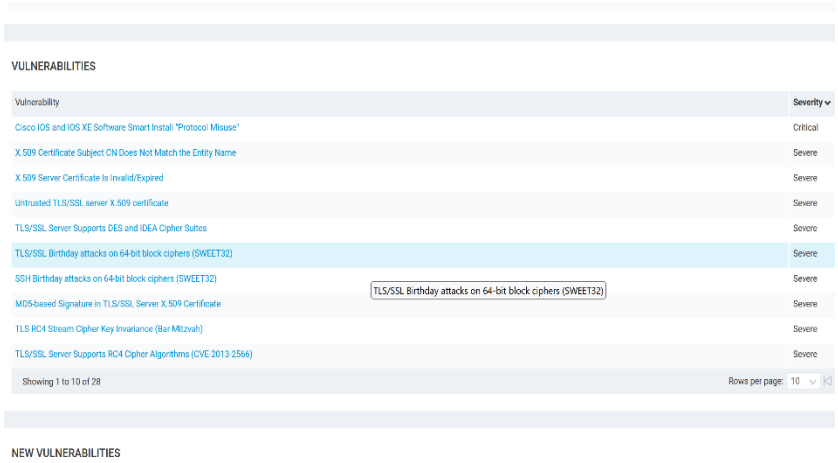


Nota. La figura muestra las vulnerabilidades por activo de la red interna de la institución.

La herramienta con ayuda de su base de datos de vulnerabilidades permite al administrador de red tener de una forma detallada cada escaneo realizado en sus activos, se muestra en la figura 104.

Figura 104

Vulnerabilidad en el software Cisco IOS.



Nota. La figura muestra detalles del software Cisco IOS.

Rapid7 nos permite detectar de igual manera los puertos de acceso y el estado en el que se encuentra configurado en cada uno de los activos de la red interna 172.253.137.201 – 172.253.137.208, observar en la figura 105.

Figura 105

Servicio de protocolos en el activo cisco 2960.

Service Name	Product	Port	Protocol	Vulnerabilities	Users	Groups	Authentication
SSH	SSH 1.25	22	TCP	6	0	0	No Credentials Supplied
Telnet	<unknown>	23	TCP	1	0	0	No Credentials Supplied
HTTP	IOS 12	80	TCP	0	0	0	Unknown
NTP	NTP	123	UDP	1	0	0	Unknown
SNMP		161	UDP	0	0	0	No Credentials Supplied
HTTPS	IOS 12	443	TCP	17	0	0	Unknown
Smart Install		4786	TCP	1	0	0	Unknown

USERS AND GROUPS

There are no users/groups to display.

DATABASES

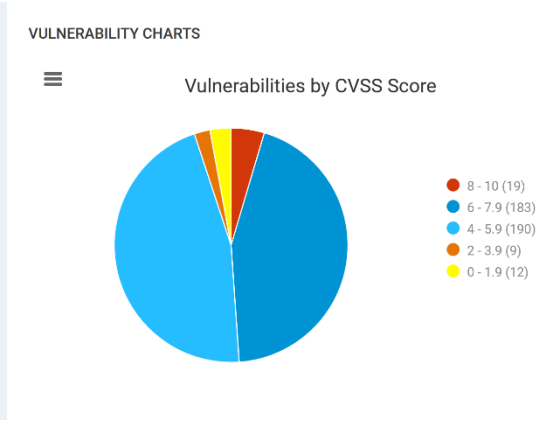
There are no databases to display.

Nota. La figura muestra los protocolos de comunicación disponible en el activo.

De manera grafica la herramienta indica el número de vulnerabilidad según su nivel de riesgo como se observa en la figura 106.

Figura 106

Modelo grafico de vulnerabilidades detectadas.

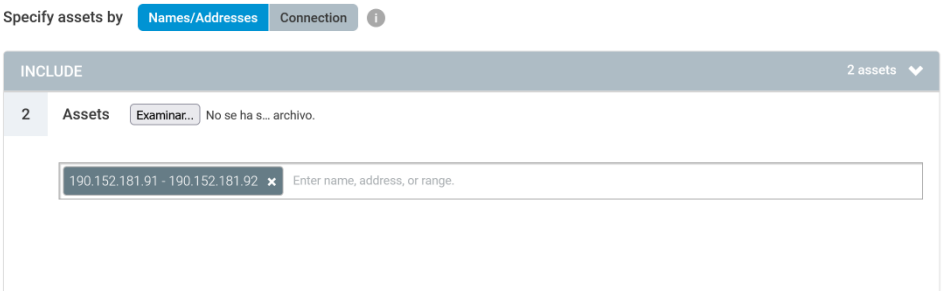


Nota. La figura muestra de manera grafica las vulnerabilidades encontradas en la red de la institución.

En la figura 107, se puede observar la creación del sitio para el análisis de los servidores de gestión de camas de la institución, los hosts 190.152.181.91 – 190.152.181.92.

Figura 107

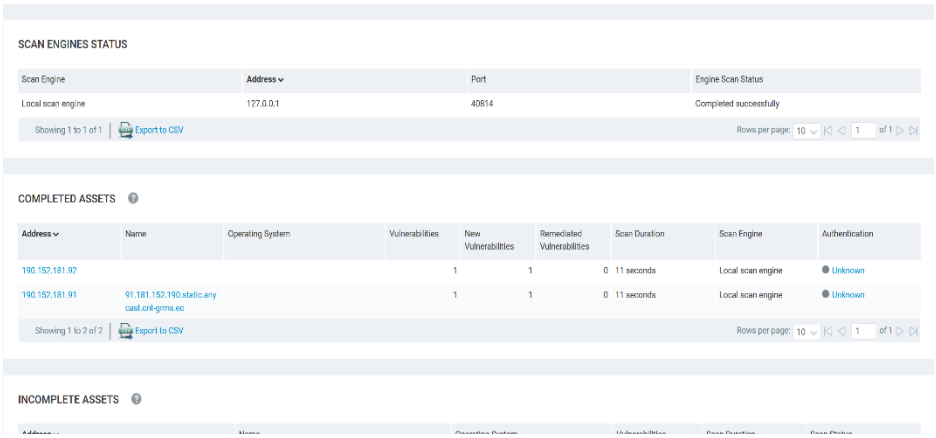
Creación de nuevo sitio de escaneo – servidores.



Nota. La figura muestra el ingreso de los activos – servidores de la institución.

Figura 108

Detección de vulnerabilidades – servidores gestión de camas.

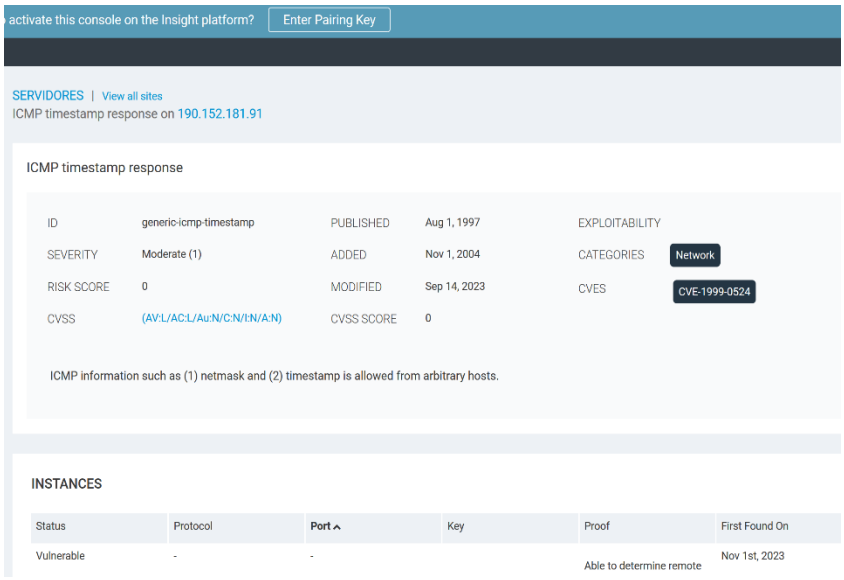


Nota. La figura muestra 1 vulnerabilidad existente en los activos, relacionada con el protocolo ICMP

En la figura 109 se observa las especificaciones detalladas del sistema instalado en el servidor host 190.152.181.91.

Figura 109

Especificaciones servidor 190.152.181.91



Nota. La figura detalla las características del servidor.

CAPÍTULO VI

PROPUESTA

Datos Informativos.

6.1. Titulo.

PROCEDIMIENTO PARA LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA PERIMETRAL EN LA INFRAESTRUCTURA DE UNA ORGANIZACIÓN.

6.1.1. Institución.

Hospital General Alfredo Noboa Montenegro.

6.1.2. Beneficiarios.

- Unidad de tecnología, principalmente su personal operativo porque podrá aplicar un procedimiento que permita garantizar la seguridad de sus activos.
- La institución con la aplicación de la Norma ISO 27001, basada en sus diferentes controles y metodologías.

6.1.3. Ubicación

- **Provincia:** Bolívar.
- **Cantón:** Guaranda.

6.1.4. Personal Responsable.

Investigador: Ing. Hugo David Peña Rosillo.
Coordinador: Ingeniero Víctor Santiago Manzano Villafuerte Magister**.**

6.2. Antecedentes de la Propuesta.

En la actualidad el uso de las comunicaciones y tecnologías es primordial en las instituciones públicas y privadas, por lo que es de gran importancia garantizar la fiabilidad de su información ante vulnerabilidades y amenazas que se pueden presentar en la infraestructura de red de la organización

Según el estudio realizado por la Policía Nacional del Ecuador y su grupo especial Interpol, detecto en base a su centro de incidentes informático y apoyado por distintas entidades de América latina determino que, el 85% de ataques a los programas informáticos son causados por error del usuario, 58% de personas dejan sus equipos tecnológicos en lugares inseguros y propensos a robos, 60% establece la misma contraseña en sus equipos tecnológicos, tarjetas de débito y crédito, 35% ha ingresado a link maliciosos enviados mediante correo electrónico, 59% hace uso del almacenamiento de información en la nube y el 80% sufre de intimidaciones en las redes sociales" (Telégrafo, 2016).

En el Ecuador las empresas u organizaciones, en su mayor parte no cuenta con una certificación de normas y políticas estandarizadas, que permitan el uso y su implementación en la infraestructura de su red en base a seguridad informática, motivo por el cual sufren ataques e infecciones de malware, ransomware ente otros afectando la integridad de sus recursos tecnológicos**.**

El Hospital Alfredo Noboa Montenegro, no cuenta con una guía o modelo de manejo ante incidentes de seguridad informática, en sus activos informáticos e infraestructura de red, motivo por el cual con el pasar de los años empiezan a presentar fallos físicos y lógicos dando lugar a la presencia de vulnerabilidades y amenazas.

Mediante el estudio se quiere contribuir en las actividades diarias en el área de TI por parte del personal de la institución HANM, con el análisis de normas, políticas y métodos de tratamiento de riesgos de incidentes informáticos, que permita establecer un modelo de buenas prácticas para su infraestructura informática.

6.3.Justificación.

Para realizar el presente estudio se basó específicamente de la recopilación de información proporcionada por el departamento de tecnologías del "Hospital General Alfredo Noboa Montenegro", para lo cual se realizó un análisis o monitoreo de sus activos con la ayuda de herramientas de escaneo como son Rapid7, NMAP y Nessus, con la finalidad de detectar las posibles amenazas y vulnerabilidades en la infraestructura de la institución y realizar las debidas medidas de mitigación de riesgos en conceptos de valoración de criticidad y su impacto que puede tener a materializarse una amenaza, proceso que se ejecutó con la aplicación de MAGERIT basándose en los controles y procedimientos de la norma ISO 27001.

Una de las debilidades que se encontró en el área de tecnologías es que no se cuenta con políticas establecidas para cada actividad que realiza su personal técnico, por lo que muchos controles y manejo de equipos tecnológicos se lo realiza de forma empírica sin una guía técnica para reaccionar ante alguna eventualidad en los activos de la institución.

El objetivo de la propuesta es estructurar un procedimiento de gestión de seguridad informática perimetral, que permita mejorar y garantizar la seguridad e integridad de la infraestructura tecnológica de sus activos para proteger su información.

6.4.Objetivos.

6.4.1. General.

Realizar un procedimiento para la gestión de la seguridad informática perimetral en la infraestructura de una organización

6.4.2. Específicos.

- Analizar normativas, estándares y modelos existentes de seguridad informática.

- Aplicar un modelo de gestión de seguridad informática para la infraestructura de una Organización.
- Validar el modelo de gestión de seguridad informática en la Institución Hospital Alfredo Noboa Montenegro.

6.5.Análisis de Factibilidad.

En la presente propuesta se consideran los siguientes tipos de factibilidad.

6.5.1. Factibilidad Operativa.

El presente proyecto es respaldado por el Gerente del "Hospital General Alfredo Noboa Montenegro", y la colaboración del personal encargado del Área de Tecnologías para la realización de pruebas, empleando los conocimientos adquiridos por el investigador.

6.5.2. Factibilidad Técnica.

Se cuenta con la infraestructura necesaria como equipos tecnológicos, software, datos e información, normas y políticas que permitan gestionar una eficiente seguridad informática perimetral de sus activos, para protección de su información.

6.5.3. Factibilidad Económica.

El proyecto es viable económicamente debido a que la elaboración de la propuesta no genera un gasto para la institución, los recursos utilizados son asumidos por parte del investigador, si en un futuro la institución requiere ejecutar la propuesta de gestión de seguridad informática perimetral, de deberá contar con una planificación de prepuesto para su implementación.

6.6. Fundamentación.

En el trabajo de investigación Almeida (2022), sobre "DISEÑO DE UN PLAN DE SEGURIDAD INFORMATICA PARA MIPYMES" trabajo que expone los riesgos a los que las MiPymes nacionales están expuestos al no contar con un plan de seguridad informática, que permita garantizar la información de sus activos, difusión de sus catálogos de servicios, teniendo como consecuencia el robo de información y acceso no autorizado a sus datos por ciberdelincuentes, llegando a una solución importante para el campo empresarial como es lo siguiente:

> Proponer a las Mi Pyme a invertir en la implementación de un plan de seguridad para la protección de la información el cual se base en la norma técnica de estandarización de políticas (NTC- ISO/IEC 27001:2013), con la finalidad de poder disminuir los riesgos mediante el aseguramiento, confidencialidad e integridad de los datos se sus sistemas informáticos.

Rodríguez (2016), define que para la implementación de un SGSI es primordial realizar una correcta gestión de riesgos en base a las vulnerabilidades presentes en los activos de información y las principales amenazas que pueden explotar estas vulnerabilidades, con la finalidad en establecer medidas preventivas y correctivas que garanticen la seguridad de la información y sus activos principales

De acuerdo con expertos en seguridad, ninguna organización puede considerarse inmune a ataques, y en base a este criterio no se trata de si sus sistemas se verán comprometidos sino cuándo y cómo sucederá (Peralvo,2023).

Según Lozada (2019), en su estudio propone el uso de la norma ISO 27001:2013, para el tratamiento de la información que manejan las empresas telefónicas en el Ecuador, en base a sus políticas y buenas prácticas que esta ofrece, además la implementación de un SERVICE DESK, que permita gestionar de una forma eficiente los incidentes y garantizar la integridad de los datos e información de sus usuarios.

6.7. Presentación del procedimiento para la gestión de la seguridad informática perimetral.

En base al proceso y al cumplimiento de cada una de las fases planteadas para el desarrollo del estudio de investigación en relación a la seguridad informática perimetral en el "Hospital General Alfredo Noboa Montenegro" específicamente en el área de tecnologías cumpliendo con las diferentes actividades realizadas y mediante la aplicación de los controles de la norma ISO 27001, se ha determinado que la probabilidad de ocurrencia de incidentes relacionados con la seguridad de sus activos es considerablemente medio y que requiere de algunas políticas correctivas para garantizar su información.

Las políticas a considerar para garantizar la seguridad informática perimetral en la infraestructura del "Hospital General Alfredo Noboa Montenegro", están definidas especialmente en el campo organizacional, lógica, física y legal, relacionadas tanto al ámbito de la seguridad de la información y el cumplimiento de los controles definidos en la norma ISO 27001.

Seguridad Organizacional.

Figura 110

Aspectos de Seguridad Organizacional.

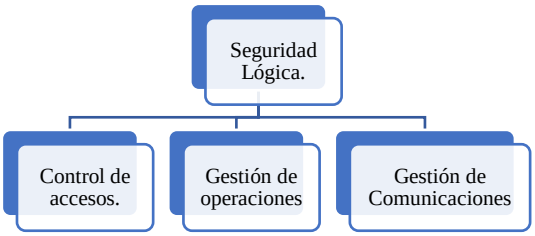
Nota. La figura muestra el proceso de seguridad organizacional en una institución.

Se definió aspectos relacionados a servicios, gestión de activos, recursos humanos y físicos, responsabilidades, así como actividades relacionadas ante incidentes que afecten la seguridad de la información de la institución.

Seguridad Lógica

Figura 111

Aspectos de Seguridad Lógica.



Nota. La figura muestra el proceso de seguridad lógica.

Seguridad Física.

Establecer políticas y controles perimetrales de seguridad para el manejo, mantenimiento y soporte técnico de equipos.

Seguridad Legal.

Se debe definir políticas y normas de seguridad, a partir de la infraestructura interna de la institución y establecer las debidas sanciones para el personal que no dé cumplimiento.

6.7.1. Definiciones.

Autenticación: Procedimiento para comprobar la identidad de un usuario al tratar de administrar un recurso tecnológico o sistema de información.

Información: grupo de datos supervisados y ordenados.

Activo de Información: componente físico o lógico que interactúa en el sistema de una institución, debe estar protegido.

Tecnologías de la Información: componente tecnológico como equipos, dispositivos inteligentes y software, centralizados en una red de datos para permitir almacenar, procesar, transferir y recuperar datos e información.

Confidencialidad: garantizar que la información no esté disponible y no pueda ser divulgada por personas no autorizadas.

Disponibilidad: proceso donde solo los usuarios autorizados tienen acceso a toda la información de la institución**.**

Integridad: garantizar que la transmisión de los datos almacenados no sufra alteraciones o perdidas**.**

Acuerdo de confidencialidad: documento que se firma entre al menos dos entidades, con un acuerdo de compartir información que no puede ser divulgada

Análisis de riego: proceso que consiste en la identificación de activos, valoración de criticidad y análisis de probabilidad e impactos de una perdida de confidencialidad, integridad y disponibilidad de la información.

Seguridad informática: Es una parte de la seguridad que se centra en la protección de los sistemas informáticos de amenazas y vulnerabilidades.

Hardware: componentes físicos de dispositivos tecnológicos.

Cifrado: proceso que se utiliza para prevenir la fuga de información mediante la técnica de criptografía, lo que permite asegurar su confidencialidad.

Control: proceso que se aplica para mitigar y evitar los riesgos.

Usuario: personas que manejan la información y administran la infraestructura tecnológica.

Amenaza: evento que una vez materializado puede causar daños lógicos o físicos en los activos.

Vulnerabilidad: son eventos que pueden ocurrir mediante una exploración a la infraestructura de red de la institución.

Centro de datos: área específica diseñada para múltiples equipos tecnológicos que se encuentran conectados a través de una red de datos.

Custodio de activo de información: es el encargado de mantener las medidas de protección sobre los activos de información que fueron definidas por la organización.

Impacto: medición de la consecuencia cuando se materializa una amenaza.

Backup: respaldos de información.

Equipo de cómputo: dispositivo electrónico que recibe un conjunto de instrucciones y que los transforma en datos numéricos u otros tipos de información.

Hacking Ético: procedimiento de actividades en una red de datos de una institución mediante un análisis penetración en los sistemas de manera y controlada sin causar daños.

Incidente de seguridad: es un evento adverso que busca vulnerar la seguridad de la información.

SGSI: Sistema de Gestión de Seguridad de la Información:

Registro de auditorías: son archivos donde se almacenan los eventos identificados en los sistemas de una red de datos de una institución.

Ataque: evento que afecta el funcionamiento de un sistema.

Passwords: clave que se asigna a cada usuario.

Licencia de software: es un contrato homologado donde el producto cuenta con todos los componentes y controles de uso e instalación.

URL: dirección web.

Software malicioso: son programas intrusivos que tienen como objetivo de introducirse en loa sistemas tecnológicos para causar daños lógicos.

Dirección IP: es un número que representa lógicamente a un dispositivo, red e interfaz, que utilizan como medio de transmisión el protocolo IP.

Terceros: son personas jurídicas o naturales que proveen servicios o productos, por ejemplos proveedore, contratistas, etc.

Dirección MAC: es un código de identificación de 48 bits (6 bloques hexadecimales), de una tarjeta de red, dispositivo tecnológico, etc.

TI: Tecnologías de la Información.

Sistema de información: conjunto de datos y operaciones donde actúan uno o más activos de información, con el objetivo de cumplir tareas de almacenamiento y procesamiento de información

Inventario de activos: es una lista documentada de los activos existentes en la institución.

6.7.2. POLÍTICAS PARA CONTROLAR LAS ACTIVIDADES RELACIONADAS CON EL USO DE TECNOLOGÍAS.

Finalidad.

La implementación de Políticas de Tecnología de la Información y Comunicación en una institución, es con el propósito de fortalecer la seguridad, explotar eficientemente los equipos tecnológicos y lo principal garantizar la protección de su información.

Ámbito.

En el campo laboral definir Políticas de Tecnología de la Información y Comunicación, permite a la institución establecer normas que deben ser

cumplidas por sus empleados, servidores y trabajadores al momento de realizar actividades de hardware, software y comunicaciones.

Responsabilidades.

El área de Tecnología de la Información será la encargada de socializar las políticas, normas, y procedimientos definidos por la institución, para su eficiente aplicación.

6.7.3. POLÍTICA PARA EL USO APROPIADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

Responsables.

Área de Tecnologías: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico.

En el "Hospital General Alfredo Noboa Montenegro", los empleados tanto internos como externos deberán llevar un uso adecuado de los recursos tecnológicos por lo que, en base a las normas y procedimientos establecidos por la institución, de debe tomar en cuenta las siguientes indicaciones.

6.7.3.1. Normas Generales.

- Para el mantenimiento de dispositivos de hardware como son impresoras, escáner, computadores y demás recursos tecnológicos de propiedad del "HGANM", el personal del área de Tecnología de la Información serán los únicos autorizados para las actividades de soporte técnico.
- Solo personal autorizado podrá acceder a las instalaciones de infraestructura tecnológica e informática.
- El personal podrá hacer uso de los equipos tecnológicos fuera de su jornada laboral únicamente si cuenta con una autorización de su jefe Superior o de Gerencia.
- El recurso tecnológico propiedad de proveedores de servicios contratados por el "HGANM", el mantenimiento de los mismos será ejecutado por su soporte técnico.

- Los empleados que tenga permisos y accesos autorizados a los sistemas informáticos del “HGANM”, no podrán hacer uso indebido de su información y datos confiables.
- Los accesos autorizados a terceros para realizar actividades en el área de Tecnologías de la Información, se registrará en un repositorio con los siguientes datos (nombres/apellidos, cédula identidad, empresa o entidad en la que labora, actividad a realizar).
- Las bases de datos y almacenamiento en servidores estarán centralizadas en el Data Center del departamento de Tecnologías de la Información.
- Se prohíbe al personal con permisos autorizados al Data Center del departamento de Tecnologías de la Información realizar actividades que no constan en la guía de acceso y manipulación de otros equipos.
- Los accesos a redes inalámbricas serán únicamente gestionados por el personal del área de Tecnologías de la información, según la necesidad del solicitante que requiera de una conexión abierta o corporativa.
- Se debe llevar un inventario actualizado de los activos tecnológicos de la institución.
- La infraestructura tecnológica del “HGANM”, tendrá un sistema operativo común, antivirus y aplicaciones autorizadas por la institución necesarias para las labores diarias, las cuales serán administradas únicamente por personal del área de Tecnologías de la Información.
- Está prohibido instalar aplicaciones no autorizadas por el personal encargado del área de Tecnologías de la Información.

6.7.3.2. Normas de Hardware.

- Diseñar un plan de mantenimiento preventivo (mensual, semestral o anual), para el correcto funcionamiento de la infraestructura tecnológica, elaborado por el personal del área de Tecnologías de la Información.
- La adquisición o arrendamiento de equipos tecnológicos será de acuerdo a las necesidades de la institución y en coordinación con el área de Tecnologías de la Información.

- Ante incidentes de robo, daño o mal funcionamiento de dispositivos de hardware del “HGANM”, estos deben ser reportados al área de Tecnologías de la Información los cuales notificaran a sus superiores o autoridades competentes.
- El personal de área de Tecnologías de la Información son los únicos autorizados para la revisión o cambio de algún componente de hardware en los equipos tecnológicos del “HGANM”.
- La revisión técnica de equipos de hardware que tenga vigente su garantía, lo realizara únicamente el personal de soporte técnico del proveedor.

6.7.3.3. Normas Data Center.

- Cumplir con la especificaciones técnicas y ambientales para el eficiente desempeño de servidore y equipos en el área de tecnologías.
- Solo personal autorizado puede ingresar al centro de datos del “HGANM”.
- La administración de los equipos, servidores sea mediante consola o conexión remota, esta únicamente autorizado para el personal del área de tecnologías.

6.7.3.4. Propiedad o derechos de la información.

- La información creada o manipulada en los sistemas, aplicaciones, correos institucionales y demás actividades de los empleados dentro de la institución son exclusivamente propiedad y responsabilidad del “HGANM”.
- Los derechos o patentes de un programa, creación de aplicaciones, documentos, artículos por uno o un grupo de empleados en las instalaciones de la institución son exclusivamente propiedad y responsabilidad del “HGANM”.
- La información que se encuentre en los equipos de cómputo de los empleados, trabajadores o servidores de la institución es exclusivamente del “HGANM”, y puede ser entregada únicamente con una autorización del jefe Inmediato o de Gerencia.

6.7.3.5.Normas para usos inadecuados.

- Instalación de software o aplicaciones en los equipos tecnológicos de la institución sin consentimiento de los responsables del área de Tecnología.
- Divulgar información confidencial de la institución en sus actividades laborales utilizando los equipos tecnológicos.
- Utilizar la infraestructura tecnológica del "HGANM", parar robo de información confidencial con fines de lucro.
- Propagación de software malicioso en la infraestructura de red sea por virus, malware, correos no deseados, etc.
- Utilizar la imagen de la institución con fines ajenos al campo laboral como puede ser acoso, difamación, calumnia, extorsión, etc.
- Ejecutar actividades que no cumplan con las normas de seguridad de la institución, afectando la integridad y eficiencia de la red de servicios del "HGANM".
- Eludir mecanismos de seguridad como acceso o permisos para acceder al área de Tecnologías.
- Hacer mal uso de los recursos tecnológicos de la institución.
- Acceder a paginas restringidas por el personal de área de tecnológicas, causando deficiencias en la red por consumo de ancho de banda del internet.
- Modificar configuraciones de software, antivirus, firewall, tarjeta de red de los equipos de cómputo, sin autorización del personal del área de tecnologías afectando el funcionamiento del desktop.

6.7.4. POLÍTICA DE CONTRASEÑAS.

Responsables.

Área de Tecnologías: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico**.**

6.7.4.1. Normas Generales.

Establecer un cumplimiento de la política de contraseña por el "HGANM", hacia su personal es de suma importancia con el fin de garantizar el acceso a

los equipos y aplicaciones de la institución únicamente a usuarios con permisos autorizados y confiables.

6.7.4.2. Normas de Administración.

- El área de Tecnología del "HGANM", creara a cada empleado un usuario y contraseña (usuario debe cambiarla por primera vez), para poder acceder a servicios de red como correo institucional, Quipux, utilización de dispositivos de salida de datos como impresiones, internet, intranet, etc**.**
- Las contraseñas son personales por lo que se prohíbe a los usuarios compartir su contraseña con terceros.
- La estructura de una clave de seguridad debe contar con palabras mayúsculas, minúsculas, números y caracteres especiales.
- El empleado debe realizar el cambio de su contraseña de usuario de red, periódicamente con un tiempo de al menos cada 30 días.
- Si el usuario a olvidado o no puede acceder con su contraseña de usuario de red deberá comunicarse o acercarse con el personal del área de tecnologías.
- Si el usuario verifica que su contraseña fue vulnerada debe comunicarse o acercarse con el personal del área de tecnologías.
- Las contraseñas de aplicaciones internas pueden contar con contraseñas independientes para su acceso.
- Los empleados deben evitar aceptar que las contraseñas se guarden automáticamente en los navegadores web.
- En caso de desvinculación de personal o cambio de rol dentro de la institución, el jefe inmediato o el área de Recursos Humanos debe notificar al departamento de Tecnología de la Información para suspender la cuenta del usuario y los accesos a la red corporativa de la institución.
- Los empleados del "HGANM" deben firmar un compromiso de responsabilidad del uso de su usuario de red y contraseña, por las actividades y procesos que puede realizar desde su usuario de red.

6.7.4.3.Prohibiciones.

- Facilitar o compartir su contraseña con terceros.
- Guardar o anotar su contraseña en archivos, correo electrónico, o cualquier otro medio de comunicación electrónica.
- Utilización de contraseñas comunes.
- Reutilización de contraseñas antiguas.

6.7.5. POLÍTICA DE USO DE CORREO ELECTRÓNICO.

Responsables.

Área de Tecnologías: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico.

6.7.5.1.Normas Generales.

- El correo electrónico institucional servirá como medio exclusivo de comunicación interna de los empleados del "HGANM".
- La información compartida en los correos electrónicos debe ser específicamente del ámbito laboral de la institución.
- Los mensajes enviados por correo electrónico institucional deben cumplir con la imagen institucional del "HGANM".
- El departamento de Recursos Humanos debe comunicar la contratación y desvinculación de personal al área de tecnologías, para que se cumpla con el proceso correcto de activación y desactivación de cuentas de usuarios.
- La información confidencial que recibe un usuario especifico mediante la red corporativa de la institución, no se debe compartir sin previa autorización del remitente.

6.7.5.2. Normas y responsabilidades del departamento de tecnologías.

- El área tecnologías tiene la facultad de difundir y capacitar las normas técnicas para el buen uso del correo institucional.

- Es responsabilidad del departamento de tecnologías del “HGANM”, capacitar al personal la forma correcta de difundir la información y datos mediante la red corporativa.
- Los servicios de correo electrónico en la institución, solamente el personal del área tecnologías está autorizado para su administración.
- Es primordial que el área de tecnología cuente con plan de mantenimiento preventivo y correctivo para el eficiente funcionamiento de la plataforma de correo electrónico de la institución.
- El departamento de Tecnología de Información y Comunicación del “HGANM”, son los únicos autorizados para la creación de usuarios, desactivación de usuarios, reseteo de claves de seguridad y otros, previa indicación del área de Recursos Humanos.
- Es responsabilidad del personal del área de tecnologías del “HGANM” proteger la plataforma de correo institucional de ataques informáticos o código malicioso.

6.7.5.3. Normas y responsabilidades de los usuarios.

- Las cuentas de usuario asignada por el área de tecnologías son exclusivas de cada funcionario para su uso laboral.
- La información compartida de su cuenta de usuario es responsabilidad del empleado de la institución.
- El usuario no debe compartir con nadie su seguridad de inicio de sesión (usuario, contraseña), con terceros.
- Los usuarios o empleados deben cumplir con las políticas de seguridad al recibir en su buzón correos no deseados.

6.7.5.4. Prohibiciones.

- No es permitido la difusión de mensajes de correo electrónico que contenga archivos ejecutables.

- Queda prohibido para los usuarios él envió de cadena de mensajes que contenga fines políticos, comerciales, religioso o de cualquiera otra índole por medio de la plataforma de correo institucional.
- El envío de mensajes que contengan contenido racista, difamatorio y ofensivo con el fin de causar daños a terceros.
- Utilizar la plataforma de correo electrónico institucional del "HGANM", con fines de ocultar o suplantar la identidad del propietario de la cuenta.
- El correo institucional no debe ser utilizado para actividades personales.
- El departamento de tecnologías tiene prohibido activar y desactivar cuentas de usuario sin previa notificación del área de Recursos Humanos.

6.7.6. POLÍTICA DE USO DE SEGURIDAD INFORMÁTICA Y DE LA INFORMACIÓN.

Responsables.

Personal de la institución: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico, funcionarios o empleados.

6.7.6.1. Normas Generales.

Las siguientes recomendaciones deben ser cumplidas por los funcionarios, empleados y servidores del "HGANM".

- No realizar modificaciones de configuración de software, hardware, básicas de los equipos ya establecidos por el departamento de Tecnologías de la Información.
- Es recomendable activar el bloqueo automático de la pantalla del computador para que no pueda ser utilizado por terceros.
- Es responsabilidad del funcionario respaldar su información de manera periódica, en discos duros extraíbles, unidades USB y otros, con el objetivo de garantizar su disponibilidad cuando el usuario lo requiera.
- No se debe realizar la instalación de aplicaciones, programas u otro software sin previa autorización del departamento de Tecnología de la Información.

- Los funcionarios no pueden realizar cambios de componentes de hardware en sus equipos de cómputo sin antes notificar al área de Tecnología de la Información.

6.7.6.2. Acuerdos de Confidencialidad.

- Los funcionarios del "HGANM", proveedores de servicios contratados u otros deben firmar compromisos de confidencialidad con el objetivo que la información de la institución no sea divulgada o mal utilizada.
- Los acuerdos de confidencialidad serán controlados y supervisados por el área de Recursos Humanos.
- Previa contratación del personal el área de Recursos Humanos socializara con el funcionario la política de confidencialidad de la institución, así como la firma del documento de compromiso adjunto al contrato laboral.

6.7.6.3.Responsables de la seguridad.

La seguridad informática de los activos de la infraestructura del "HGANM", está a cargo del departamento de Tecnología de la Información y Comunicación.

6.7.6.4.Responsables de la Información.

- Los responsables directos de la información son los que cuentan con la potestad para crear, manejar y comunicar el tipo de información de sus sistemas aplicativos y son las Gerencia, Dirección y Responsables de aérea.
- Los responsables secundarios de la información son aquellos que pueden acceder, modificar, almacenar y compartir información, que fue autorizada por su jefe superior.
- Los custodios de información son los empleados de la institución, cuales deben dar cumplimiento a los acuerdos de confidencialidad para cuidar, respaldar y almacenar la información de la institución.

6.7.6.5.Clasificación de la Información.

- Los propietarios de la información son responsables del monitoreo y supervisión periódicamente de la clasificación de sus activos según su nivel de confidencialidad.
- La información debe ser etiquetada de acuerdo a la clasificación otorgada la misma que tiene que ser clara y visible.
- Toda información generada en la institución y que no se encuentre debidamente etiqueta y sin cumplir los lineamientos de clasificación de la información, será considerada como información PRIVADA.
- La información que por naturaleza puede ser visible y divulgada sin afectar en ningún sentido la integridad de la institución es considerada información pública.
- La información confidencial de uso solamente interno para el personal especifico previo a permisos y autorización para su manejo.

6.7.6.6. Respaldo de Información.

- Los funcionarios deben cumplir con los lineamientos y procedimientos internos para la generación, almacenamiento y tratamiento de las copias de información, garantizando su integridad y confidencialidad.
- Los funcionarios deben identificar de sus activos tecnológicos la información y clasificar su información de acuerdo a su nivel de criticidad e importancia.
- El departamento de tecnologías debe capacitar a los funcionarios para el resguardo de información en medios de almacenamiento físico, nube institucional que permita el acceso rápido y eficiente a su información resguardada.

6.7.6.7.Recursos Compartidos.

- El acceso a carpetas compartidas se tiene previo la autorización de permisos del propietario de la información para acceder a su equipo de cómputo o servidor.

- Se debe definir el tipo de acceso y roles (escritura – escritura/ lectura), necesarios para las actividades a realizar en una carpeta compartida.
- Para el manejo de información confidencial de la institución la creación de carpetas compartidas se debe almacenar en el servidor de archivos.
- Los funcionarios de la institución podrán acceder a las carpetas compartidas del servidor de archivos, si cuenta con permisos autorizados previa justificación de las actividades a realizar.

6.7.7. POLITICA DE USO DE SOFTWARE.

Responsables

Área de Tecnología: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico.

6.7.7.1. Normas de administración.

- El área de Tecnología de la Información del "HGANM", son los encargados del manejo, instalación, soporte y funcionamiento eficiente de los recursos tecnológicos.
- Utilizar software licenciado para el sistema operativo de los equipos de cómputo.
- Revisar periódicamente la vigencia o caducidad de las licencias adquiridas.
- Establecer procedimientos y estándares para el uso de software.
- El departamento de Tecnologías establecerá responsabilidades y procedimiento para controlar la instalación de software operativo.
- El departamento de Tecnologías evaluara y analizar si es adecuado actualizar las versiones del software en sus equipos sin causar afectación o daños lógicos.

6.7.7.2. Prohibiciones.

- Instalación de copias o software sin licencia.
- Instalar software descargado de páginas web con virus.
- Instalación de programas o software en los equipos de cómputo sin notificar al área de Tecnologías.

6.7.7.3.Requerimientos.

- Los usuarios podrán requerir la instalación de un programa o software especifico, únicamente al área de Tecnologías.

6.7.8. POLÍTICA DE USO DE INTERNET E INTRANET.

Responsables.

Área de Tecnología: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico.

6.7.8.1. Normas Generales.

Los servicios de internet e intranet, son las herramientas de consulta de información, investigación, así como el medio de conexiones de los sistemas aplicativos de la institución, facilitando la ejecución de las labores diarias.

- El departamento de Tecnologías, debe evaluar si la institución cuenta con el recurso tecnológico necesario y óptimo para la prestación del servicio de internet e intranet.
- El uso del servicio de internet e intranet en la institución está condicionado para fines propios de actividades laborales.
- Para que los usuarios puedan acceder a un sitio web restringido, debe solicitar al departamento de Tecnologías la habilitación del sitio, adjunto la justificación y actividades a realizar en el sitio web.
- El área de tecnologías debe aplicar un monitoreo constante del servicio de internet, para evitar lentitud y deficiencia del servicio.
- El departamento de tecnología debe establecer políticas y controles para evitar la descarga de programas y software no autorizado.
- El intercambio de información de la institución entre funcionarios se lo realizara por medio de la red local, intranet o VPN.

6.7.8.2. Normas de responsabilidad para el personal

- El área de tecnologías es responsable del monitoreo del uso del internet e intranet, supervisando el cumplimiento de políticas y normas que protejan la confidencialidad de la información.
- Los funcionarios, empleados o servidores de la institución son los responsables del envío de mensajes, archivos o programas a través de internet o intranet.
- El departamento de tecnologías de la Información es el único que se encargara de resolver problemas técnicos de conexión de internet en los recursos tecnológicos del "HGANM".
- El proveedor del servicio de internet y de datos de la institución es responsable de garantizar el ancho de banda y su disponibilidad.
- El proveedor de servicio de internet y de datos es el encargado de brindar el soporte técnico adecuado ante fallas técnicas, fibra óptica o equipos.

6.7.8.3.Prohibiciones.

- Los funcionarios no deben descargar software, programas u otros que contengan código malicioso, spam, malware y virus.
- Los funcionarios no pueden acceder a paginas relacionadas como pornografía, drogas, hacking u otras páginas que vayan contra la ética moral de la institución.
- Utilizar el servicio de internet o de intranet con fines negativos de afectar la imagen del "HGANM".
- Los funcionarios tienen restringido el acceso a paginas como redes sociales Facebook, YouTube, etc.
- Está prohibido descargar música, videos, películas u otro material ajeno actividades laborales de la institución.
- Difundir spam ocasionado por recibir correos no deseados, produciendo lentitud en el servicio de internet.

6.7.9. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD.

Responsables.

Área de Tecnología: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico.

6.7.9.1. *Normas Generales.*

- Los propietarios de los activos tecnológicos de la institución deben comunicar al área de Tecnología de la Información, si en sus activos presentan algún incidente de seguridad para su revisión.
- El área de Tecnología de la Información realizara las actividades de soporte técnico ante incidentes de seguridad reportado por los funcionarios del "HGANM".
- El departamento de Tecnología clasificará los incidentes de seguridad por nivel de criticidad, tratando como prioridad los incidentes de nivel crítico y deberá comunicar a Gerencia, Dirección o jefe Inmediato.
- Los funcionarios deben reportar inmediatamente si detecta que algún activo tecnológico no trabaja eficientemente o presenta algún incidente de seguridad.
- El área de Tecnología debe manejar una base de datos con toda la información de los incidentes de seguridad reportados, con la finalidad de mejorar el tiempo de reacción y solución para incidentes futuros.
- La institución debe capacitar periódicamente a su personal del área de Tecnología, para el manejo adecuado de los incidentes de seguridad, causas, tratamiento y soluciones.
- El área de Tecnología debe crear medidas de seguridad eficientes para proteger los activos de información.
- Es responsabilidad del departamento de Tecnología, realizar un análisis de la infraestructura tecnológica de la institución para encontrar las debilidades de seguridad que causan y contribuyen al incidente.

6.7.10. POLÍTICA DE SEGURIDAD FÍSICA Y MEDIOAMBIENTAL.

Responsables.

Área de Tecnologías de la Información y Comunicación, Gerencia, Dirección y funcionarios de la institución.

6.7.10.1. Normas generales.

- El departamento de tecnologías debe desconfigurar o cambiar de forma inmediata los privilegios de acceso a la cuarto de comunicaciones y activos bajo custodia, cuando un funcionario es desvinculado de las actividades laborales.
- Es responsabilidad del área de tecnología que los activos tecnológicos del centro de datos se encuentren protegidos ante vulnerabilidades o fallas de interrupciones eléctricas.
- Las solicitudes para los permisos de acceso a cuarto de comunicaciones son únicamente aprobados por el área de tecnologías.
- Los permisos de acceso a la data center de la institución para los proveedores de servicios contratados serán autorizados por el área de tecnología previa justificación de las actividades a realizar por su personal.
- El departamento de Tecnologías debe proveer su cuarto de comunicaciones en condiciones medioambientales como el control de temperatura, sistema de detección de incendios, alarmas, sistemas de videovigilancia y monitoreo para garantizar la funcionalidad de sus activos.
- El área de tecnología debe elabora y plan de contingencia de mantenimiento de redes eléctricas, cableado de red de datos, infraestructura de voz y otros, mediante la contratación de personal capacitado para su ejecución.
- El personal de empresas de servicios contratados debe utilizar prendas distintivas, credencial u otros que faciliten su identificación.
- Los pasantes que realicen sus actividades en el centro de datos deben llevar una bitácora donde se registre las actividades desarrolladas previa supervisión del personal del área de tecnología.

6.7.11. POLÍTICA DE CRIPTOGRAFÍA.

Responsables.

Área de Tecnología: Analista de Tecnología de la Información y Comunicación – Analista de Soporte Técnico.

6.7.11.1. Normas Generales.

- Establecer métodos criptográficos como firma electrónica, autenticación y cifrado, con la finalidad de proteger la información sensible ante riesgos de confidencialidad, disponibilidad e integridad.
- La institución "HGANM", deberá proponer un plan de controles criptográficos para proteger la información y ciclo de vida de las claves criptográficas.
- El área de Tecnologías de la Información definirá el mejor método de cifrado que se adapten a las especificaciones técnicas de la herramienta a utilizar.
- Las claves criptográficas pueden mantenerse en los equipos mientras estos se encuentren funcionando y cumpliendo las medidas de seguridad adecuada.
- En la protección de claves criptográficas que requieran encriptación, se asignara una protección adecuada en los equipos utilizados para generar, almacenar y archivar claves privadas.
- Para la protección de firmas y certificados digitales avanzados, su almacenamiento se realizará en equipos con características de seguridad de hardware.
- La utilización de claves criptográficas será en un plazo concreto o periódico.
- Se debe analizar el cumplimiento y revisión de la ejecución de esta Política de manera mensual, semestral o anual según coordinación del área de Tecnología.

6.7.12. POLÍTICA DE PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES.

En cumplimiento de la Constitución de la Republica del Ecuador en el art 66, literal 19, establece en garantizar el derecho de protección y el acceso a información y datos de carácter personal. El "Hospital Alfredo Noboa Montenegro" a través del área de Tecnología y en cumplimiento de la Política garantizara la protección de los datos personales de los funcionarios, empleados o servidores.

Responsables.

Área de Tecnologías de la Información y Comunicación, Analista de soporte técnico, y funcionarios de la institución.

6.7.12.1. Normas Generales.

- Las áreas encargadas de procesar los datos personales de funcionarios o servidores de la institución "HGANM", deben tener una autorización para utilizar, compartir, circular y actualizar dichos datos personales en el desarrollo de las actividades de la institución.
- El departamento de Tecnologías tiene la responsabilidad de establecer los controles necesarios para proteger la información de los funcionarios de la institución para evitar su divulgación, alteración o mal uso de la misma.
- Los funcionarios a utilizar la plataforma o sistemas de información de la institución, deben manejar de manera responsable su calve de acceso y realizar cambios periódicos de la misma.
- El departamento de Tecnologías debe emplear controles de seguridad en los equipos de cómputo o redes privadas, para que los funcionarios puedan acceder a la plataforma o sistemas de información de la institución
- El área de Tecnologías debe definir protocolos de seguridad de estricto cumplimiento, que garanticen que los funcionarios con acceso a datos personales, no puedan divulgar esta información.