ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DESARROLLAR UN PLAN DE MEJORA A LA SEGURIDAD DE LA INFRAESTRUCTURA DE LA RED DEL ÁREA DE TI, PARA UNA INSTITUCIÓN EDUCATIVA DE TERCER NIVEL”

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. JOHANNA FIERRO FARIÑO

ING. JOSUÉ SÁNCHEZ BUENAÑO

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Quiero expresar mi agradecimiento, primero a Dios, por brindarme la oportunidad de cursar esta Maestría. A mi mamá y a toda mi familia, les debo un agradecimiento especial por su comprensión y apoyo incondicional durante todo el proceso de estudio.

Mi sincero agradecimiento también a Daniel y Reina, quienes me motivaron a unirme al grupo de estudios. A Telconet S.A., extiendo mi profunda gratitud por el apoyo brindado para el desarrollo y culminación de esta Maestría.

Agradezco a todos los profesores que, con sus valiosas experiencias y conocimientos, enriquecieron mi formación académica. Finalmente, quiero destacar el apoyo de mi amigo y compañero de titulación, Josué, cuya colaboración hizo que este recorrido académico fuera mucho más gratificante y enriquecedor.

Ing. Johanna Fierro Fariño

En primer lugar, agradezco a Dios, cuya guía y fortaleza me han permitido avanzar y culminar con éxito este importante paso en mi formación académica.

A Telconet S.A., expreso mi más profundo agradecimiento por el apoyo brindado a lo largo de este proceso, lo cual fue fundamental para lograr un equilibrio entre mis responsabilidades profesionales y académicas.

A mi familia, les agradezco sinceramente por su amor incondicional, su comprensión y por ser mi mayor fuente de motivación en todo momento.

A mis tutores, les expreso mi gratitud por su invaluable orientación, dedicación y conocimientos, que han sido clave en la elaboración de este trabajo.

Finalmente, quiero agradecer de manera especial a mi compañera de tesis, Johanna Fierro, por su colaboración, compromiso y apoyo durante todo este recorrido académico.

Ing. Josué Sánchez Buenaño

DEDICATORIA

Este trabajo de titulación está dedicado con todo mi corazón a mi familia, quienes son mi pilar fundamental. A mis seres queridos que, aunque ya no están físicamente, continúan cuidándome desde el cielo, especialmente a mi papá.

A mis hermanas, quienes la vida me ha regalado, les agradezco profundamente por su constante presencia y apoyo. Su aliento y motivación han sido esenciales para que pudiera superar los desafíos y concluir este proceso.

Gracias por celebrar cada uno de mis logros como si fueran propios. Su amor y dedicación me han dado la fuerza para seguir adelante. Los amo un mundo.

Gracias siempre.

Ing. Johanna Fierro Fariño

Dedico este trabajo de titulación, en primer lugar, a Dios, porque gracias a Él soy lo que soy, y cada triunfo en mi vida ha sido por su gracia inmerecida.

A cada uno de mis familiares, quienes siempre han estado a mi lado, brindándome su apoyo y consejos, ayudándome a ser una mejor persona. A mis padres, Jorge y Sandra, porque siempre se sacrificaron para que nunca me faltara nada.

Con profundo amor, también dedico este trabajo a mi abuelita Norma. Aunque ya no está conmigo, sé que se habría sentido orgullosa del hombre en el que me he convertido gracias a sus sabios consejos.

Finalmente, a mi querida esposa, Michelle, quien siempre ha estado allí para apoyarme y celebrar cada uno de mis triunfos como si fueran suyos. Y no podrían faltar mis adorables hijos, Nathan y Abbie, que son mi fuente de motivación.

Ing. Josué Sánchez Buenaño

TRIBUNAL DE SUSTENTACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

M.SC. LENIN EDUARDO FREIRE COBO

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

M.SC. JUAN CARLOS GARCÍA PLÚA

REVISOR

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.”

ING. JOHANNA ALEXANDRA FIERRO FARIÑO

ING. JOSUÉ DAVID SÁNCHEZ BUENAÑO

RESUMEN

El objetivo principal de este trabajo de titulación es la creación de políticas de seguridad que formen un Plan de Mejora a la Seguridad que debe implantarse en la Institución de Tercer Nivel de la ciudad de Guayaquil.

Los conceptos más relevantes a la seguridad de la información son enunciados y descritos de manera concisa en el marco teórico, la metodología descriptiva se ha usado como base para el desarrollo del Plan de Mejora de Seguridad.

A través del levantamiento de información realizado, se pudo conocer de una manera más detallada los activos de información y la manera en que son tratados basándonos en los hallazgos encontrados durante la entrevista, encuestas y hacking ético se realizó la creación de las políticas y procedimientos.

Posteriormente, se presentan las respectivas conclusiones y recomendaciones que fueron aplicadas.

ÍNDICE GENERAL

ABREVIATURAS

AP	Punto de Acceso
CNT	Corporación Nacional de Telecomunicaciones
CPE	Equipo Local del Cliente
DNS	Sistema de Nombres de Dominio
IDS	Sistema de Detección de Intrusiones
IPS	Sistema de Prevención de Intrusiones
ISO	Organización Internacional de Normalización
MFA	Múltiples Factores de Autenticación
NMAP	Rastreador de Red
PMI	Instituto de Gestión de Proyectos
SGSI	Sistema de Gestión de Seguridad de la Información
SMB	Bloqueo de Mensajes de Servidor
SNMP	Protocolo Simple de Administración de Red
SO	Sistema Operativo
TI	Tecnología de la Información
UPS	Sistema de Alimentación Ininterrumpida
USB	Bus Serie Universal
WAF	Firewall de Aplicaciones Web
Wi-Fi	Fidelidad Inalámbrica

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En la actualidad todo tipo de institución a nivel mundial, sin importar su tamaño hace uso de los sistemas tecnológicos para el tratamiento de su activo más importante, la información, sin embargo, no todas las instituciones están conscientes de las diversas amenazas que pueden llegar a hacer mal uso de la información; y una de las causas principales es el no contar con controles de seguridad que permitan mantener la integridad, disponibilidad y confidencialidad.

En la nueva era digital y de cara a los retos cada vez más complejos para garantizar la tranquilidad de las personas en este nuevo mundo, la seguridad de la información se ha convertido en un indispensable para las diversas esferas que existen, desde la pública en los gobiernos hasta la privada, en las empresas [1].

Las instituciones educativas no son la excepción, estos tratan información muy importante de sus estudiantes, personal docente, administrativo, etc. mediante los sistemas tecnológicos. En muchas ocasiones, los usuarios son los responsables de que se materializan los diversos incidentes de seguridad, como lo son los accesos no autorizados, fuga y modificación de información, ya que ellos son los más vulnerables y no tienen conocimiento sobre las consecuencias que esto puede acarrear.

El acceso no autorizado a los sistemas e infraestructura de una empresa sigue siendo un tema fundamental en su operación diaria. Aunque con el avance e incorporación de nuevas tecnologías, las compañías han sumado nuevos sistemas de manejo de identidad y control de ingreso tanto físicos (biométricos, claves, tarjetas de proximidad, etc.) como digitales (múltiples factores de autenticación o MFA) para mejorar su seguridad [2].

Por tal motivo, con la realización de este trabajo de titulación se busca implementar controles de seguridad siguiendo la norma internacional ISO/IEC 27002:2013 dominio A9 y A11, que ayuden a establecer medidas de seguridad sobre los usuarios, un

correcto uso de sus contraseñas, limitar el acceso a los sistemas de tratamiento de información y protección de las áreas seguras con controles de entrada adecuados.

CAPÍTULO I

GENERALIDADES

1.1. ANTECEDENTES

La Institución Educativa de Tercer Nivel es un centro de educación superior ubicado en la ciudad de Guayaquil, Ecuador. Es una de las universidades más antiguas y prestigiosas del país. La institución ofrece programas de estudio en diversas áreas, incluyendo ciencias sociales, humanidades, ciencias naturales, tecnología, negocios, derecho, medicina, y más.

La pandemia de COVID-19 ha tenido un impacto significativo en la educación superior en todo el mundo tal es así; que, en Ecuador durante la pandemia, las universidades tuvieron que adaptarse rápidamente a nuevos desafíos y cambios en la forma en que brindan educación. La educación en línea fue el recurso más utilizado, aunque no tan desarrollado. Las universidades vieron la necesidad de

invertir en tecnología y capacitación para ofrecer programas en línea de calidad, ya que esta modalidad se volvió esencial en situaciones de emergencia como la pandemia.

En estas inversiones deben considerarse de manera particular la Seguridad Informática ya que, los ciberataques y amenazas cibernéticas aumentaron significativamente y con ello la necesidad de implementar medidas que los contrarresten.

La institución no posee ningún tipo de control de seguridad informática sobre las redes y tampoco poseen procesos ni políticas de control de acceso, para sus sistemas lo que genera un riesgo enorme para la información de la institución como de todos sus relacionados. Adicional no tienen conciencia de todas amenazas cibernéticas a las que están expuestos.

1.2. DESCRIPCIÓN DEL PROBLEMA

Hoy en día, a nivel global, las organizaciones públicas y privadas cuentan con redes locales para transmitir su información. El creciente desarrollo de la tecnología de la información ha hecho que instituciones educativas, empresas y gobiernos estén ansiosos por ser parte de este desarrollo, pero esto conlleva también a que en los últimos años ha habido una gran cantidad de ataques de piratas informáticos dirigidos a los usuarios de las redes informáticas.[1]

Tras el Covid, los ciberataques aumentaron sobremanera porque la virtualidad tuvo el protagonismo para el desarrollo de la nueva realidad que nos tocó vivir. La falta de medidas de seguridad en las redes, especialmente en los servicios de Internet, convirtió a Latinoamérica en el blanco perfecto para los ingresos no autorizados que además no solamente buscaban demostrar la fragilidad de las redes sino también lucrar de estas vulnerabilidades.[2]

Las vulnerabilidades se han vuelto relativamente fáciles de detectar, además que se publican en la dark web o en grupos de Telegram, tal como sucedió en Colombia el 2022 cuando el grupo ransomware RansomHouse atacó a Keralty.[3]

Aunque las empresas e instituciones educativas en Ecuador dependen cada vez más de las redes informáticas, la ausencia de una educación continua en ciberseguridad hizo que solo se la considere como una opción y no un requisito. Con la visibilidad de los ataques que se ejecutaron a varias empresas ecuatorianas como, por ejemplo: Banco del Pichincha, CNT y Municipio de Quito, que son empresas privadas y públicas, mismas que vieron afectadas sus labores normales. A nivel Empresarial se comenzó a crear una consciencia sobre lo que implica tener un Plan de Seguridad Informática.[2]

La Institución Educativa de Tercer Nivel posee una red de área local con sus respectivos servicios, a la cual no se la ha sometido a ninguna técnica de “hacking ético” para detectar vulnerabilidades. Esto representa un alto riesgo de seguridad porque ponen en un severo peligro la información, la misma que puede ser alterada o en el peor de los casos robada en su totalidad. Esto ocasionaría un impacto muy grande tanto en sus operaciones laborales como en su prestigio educativo.

El Gerente Informático de la Institución Educativa de Tercer Nivel está en total disposición de que se ejecute el hacking ético. Porque es un proceso inexistente dentro de su red, y considera importante el conocimiento de sus vulnerabilidades y, sobre todo, el tema de cómo remediarlas para así brindar sus servicios de manera segura con la debida protección de los datos que involucran su desempeño laboral.

1.3. SOLUCIÓN PROPUESTA

Esta propuesta plantea la creación de un Plan de Mejora que, mediante el conocimiento de las vulnerabilidades informáticas en la red del Departamento de TI de la Institución Educativa de Tercer Nivel, realizará las correcciones respectivas para contribuir con un funcionamiento más acorde a los estándares de la Seguridad Informática.[4]

En la Institución Educativa se utiliza la red como herramienta de trabajo diaria y se comparte información sobre procesos internos; es un riesgo muy alto que la red carezca de protecciones de seguridad, ya que tienen una exposición alta a los ciberataques.

Por lo tanto, previo a la creación del plan se ejecutará un hacking ético para evidenciar todas las vulnerabilidades existentes en las redes, las mismas que permitirán el trazado de los procesos de seguridad informática que se necesitan implementar en la institución educativa. La práctica del hacking ético se refiere al uso de técnicas y herramientas para identificar vulnerabilidades y debilidades en sistemas y redes informáticas.[5] En el caso de la Institución Educativa, implica analizar la seguridad de la red y sus dispositivos, buscando debilidades que podrían ser explotadas por atacantes malintencionados.[6]

En base a los hallazgos encontrados se podrá establecer un Sistema de Gestión de Seguridad de la Información (SGSI), cumpliendo así con los estándares internacionales que exige la Norma ISO 27001.[7]

Con este Plan de Seguridad Informática se busca reducir los ataques y la pérdida de información que pueden causar graves problemas tanto al desarrollo de las actividades diarias de la Institución Educativa como al prestigio de esta.[8]

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL

Desarrollar un plan de mejora a la seguridad de la infraestructura de la red, usando herramientas de pruebas de vulnerabilidades (hacking ético) para una institución educativa de tercer nivel.

1.4.2. OBJETIVOS ESPECÍFICOS

Identificar las brechas en la seguridad de la red a través de la evaluación al personal de TI usando encuestas.

Determinar los posibles puntos de acceso vulnerables en la red mediante hacking ético.

Desarrollar un plan para mejorar la Seguridad en la Infraestructura Informática de la red.

1.5. METODOLOGÍA

El alcance es del tipo descriptivo, dado que nuestro proyecto busca identificar vulnerabilidades en la infraestructura de la red de una institución educativa de tercer nivel utilizando herramientas para realizar hacking ético y pruebas de penetración. Es un estudio no experimental del tipo transversal en el que usaremos herramientas de código libre para vulnerar la red y descubrir cada uno de los fallos en la Seguridad Informática de esta red.

El tipo de muestreo que utilizaremos en nuestro estudio será no probabilístico y por conveniencia, ya que en el área donde queremos desarrollar nuestro proyecto conocemos y tenemos empleados identificados que pueden aportar con información relevante.

El área de TI, que será el foco de este trabajo, emplea a 33 profesionales informáticos, incluyendo personal responsable de desarrollo, infraestructura y soporte académico. Por este motivo, utilizamos como tipo de instrumento una encuesta, la cual constará de un formulario en línea de 20 preguntas, que nos permitirá conocer si los empleados encuestados tienen conocimientos básicos acerca de la Seguridad de la Información, conocimiento de las vulnerabilidades informáticas a las que está expuesta su red y sobre los beneficios que nos brinda el realizar un Hacking Ético.

Con los resultados de la encuesta se espera conseguir una idea sobre las brechas de seguridad existentes en la red que nos encaminen sobre el hacking ético que debemos ejecutar e ir hilvanando las bases del Plan de Seguridad de Información.

Finalmente, utilizaremos la metodología de Project Management Institute (PMI), la cual nos permitirá realizar el Hacking Ético por etapas. A continuación, se detalla cada una de ellas:

Inicio: Obtener información tanto de la infraestructura de red como del personal de TI para el inicio del proyecto.

Planificación: Analizar la infraestructura de la red de la institución educativa para el diseño de las pruebas y test de penetración.

Ejecución: Se ejecutará el análisis de las vulnerabilidades y pruebas de penetración mediante el software de hacking.

Control: Evidenciar el resultado obtenido en cada una de las pruebas realizadas mediante la elaboración de un reporte.

Cierre: Se presenta el informe con las vulnerabilidades identificadas y el plan para mejorar la seguridad de la información de la institución educativa.

CAPÍTULO II

MARCO TEÓRICO

A continuación, se realizará una descripción de los conceptos teóricos sobre los temas inherentes en el desarrollo del presente proyecto, tales como: Plan de Seguridad y el Hacking ético.

2.1. PLAN DE SEGURIDAD.

Un Plan de Seguridad Informática es un conjunto de políticas, procedimientos y reglas creados para proteger los activos de información de una organización, tales como sistemas informáticos, redes, datos y recursos digitales, de amenazas y riesgos potenciales. Tiene como objetivo principal garantizar la

confidencialidad, integridad y disponibilidad de los datos y sistemas de una organización.

Un Plan de Seguridad Informática posee algunos componentes clave como los siguientes:

- **Evaluación de riesgos:** Realizar una evaluación exhaustiva de los riesgos que enfrenta la organización en términos de seguridad informática. Esto implica identificar las amenazas, vulnerabilidades y posibles impactos en caso de incidentes de seguridad.
- **Políticas de seguridad:** Establece políticas y directrices claras que definen cómo se deben proteger los activos de tecnología de la información. Esto incluye políticas de contraseñas, políticas de acceso, políticas de cifrado y otras normativas relacionadas con la seguridad.
- **Procedimientos y controles:** Define los procedimientos y controles específicos que deben implementarse para mitigar los riesgos identificados. Esto puede incluir la configuración de cortafuegos, el monitoreo de eventos de seguridad, la gestión de parches y la respuesta a incidentes.
- **Educación y capacitación:** Promueve la concienciación sobre la seguridad informática entre los empleados y proporciona capacitación para garantizar que comprendan y sigan las políticas y procedimientos de seguridad.
- **Gestión de acceso:** Establece mecanismos de control de acceso para garantizar que solo las personas autorizadas tengan acceso a sistemas y datos confidenciales.

- **Protección contra malware:** Implementa soluciones de seguridad, como antivirus y antimalware, para detectar y prevenir la propagación de software malicioso.
- **Actualizaciones y parches:** Asegura que los sistemas y software se mantengan actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas.
- **Respuesta a incidentes:** Define un plan de respuesta a incidentes que describe cómo la organización abordará y mitigará las amenazas y los incidentes de seguridad en caso de que ocurran.
- **Auditoría y revisión:** Establece un proceso continuo de auditoría y revisión para evaluar la efectividad de las medidas de seguridad y realizar mejoras según sea necesario.
- **Cumplimiento:** Asegura que el plan cumple con las regulaciones y estándares de seguridad aplicables, como la ISO 27001.

Un Plan de Seguridad Informática es esencial para proteger los activos digitales de una organización y mitigar los riesgos asociados con las amenazas cibernéticas en constante evolución. Además, debe ser revisado y actualizado de manera regular para adaptarse a los cambios en la tecnología y las amenazas emergentes.

2.2. HACKING ÉTICO.

El hacking ético, también conocido como "hackeo ético" o "hacker ético", se refiere a la práctica de utilizar habilidades y conocimientos avanzados en informática y seguridad informática de manera legal y ética para identificar y solucionar vulnerabilidades en sistemas informáticos y redes. Los hackers

éticos, a menudo denominados "white hats", trabajan con el permiso y la cooperación de los propietarios de los sistemas o redes que están evaluando. Sus actividades tienen como objetivo mejorar la seguridad de estos sistemas, en lugar de dañarlos o explotarlos con fines maliciosos.

2.2.1. TIPOS DE HACKERS

Sombrero Blanco (White Hat)

Estos son hackers que utilizan sus habilidades para identificar vulnerabilidades en sistemas informáticos con el permiso del propietario, con el objetivo de fortalecer la seguridad de esos sistemas. Trabajan de manera legal y ética, y su labor es crucial para proteger la seguridad en línea.

Sombrero Negro (Black Hat)

Los hackers maliciosos son aquellos que utilizan sus habilidades con fines delictivos o destructivos, como robar datos, cometer fraudes, difundir malware o realizar ciberataques. Sus acciones son ilegales y pueden causar daño a individuos, empresas o instituciones.

Sombrero Gris (Grey Hat)

Estos hackers se sitúan en un punto intermedio entre los hackers éticos y los maliciosos. A menudo realizan acciones sin el permiso explícito del propietario, pero su intención puede variar y puede ser cuestionable en términos de ética.

Sombrero Verde (Green Hat)

A veces se usa este término para referirse a hackers que carecen de la experiencia o habilidades avanzadas de los white hats, pero que están dispuestos a ayudar a resolver problemas de seguridad informática.

2.2.2. FASES DE UN HACKING ÉTICO

Reconocimiento

En esta fase inicial, el hacker ético recopila información sobre el objetivo, como direcciones IP, nombres de dominio, rangos de red, tecnologías utilizadas, y cualquier otra información pública relevante. Esto ayuda a comprender el alcance de la evaluación.

Escaneo

En esta etapa, se utilizan herramientas de escaneo de seguridad para identificar activos en la red y buscar posibles vulnerabilidades. Esto puede incluir el escaneo de puertos, la identificación de servicios en ejecución y la búsqueda de puntos débiles conocidos.

Enumeración

Una vez finalizado el escaneo, se procede a enumerar e identificar la información que se llegó a escanear, por ejemplo, hosts, S.O, usuarios, etc.

Análisis de Vulnerabilidades

Una vez identificadas las vulnerabilidades, se realiza un análisis más detallado para comprender su gravedad y cómo podrían ser explotadas. Se verifica la existencia de vulnerabilidades y se evalúa su impacto.

Explotación

En esta fase, se intenta explotar las vulnerabilidades encontradas para verificar si son realmente aprovechables. Esto se hace con el permiso del propietario del sistema y siguiendo las mejores prácticas éticas.

Informe

Una vez completada la evaluación, se prepara un informe detallado que describe las vulnerabilidades encontradas, sus impactos potenciales y recomendaciones para su corrección. Este informe se comparte con el propietario del sistema para que puedan tomar medidas correctivas.

CAPÍTULO III

LEVANTAMIENTO DE INFORMACIÓN

3.1. EVALUACIÓN AL PERSONAL DE TI MEDIANTE ENCUESTA PARA IDENTIFICAR BRECHAS EN LA SEGURIDAD DE LA RED

Durante la recopilación de información, realizamos entrevistas y encuestas al personal de TI para determinar si tenían una comprensión básica de la seguridad de la información, de las vulnerabilidades informáticas a las que está expuesta su red Wi-Fi y sobre los beneficios que nos brinda un Hacking Ético.

Con el objetivo de comprender las brechas de seguridad existentes en la red que nos encaminen sobre el hacking ético que debemos ejecutar, además de entrevistar al Administrador Jefe de TI, se realizó una encuesta de 20 preguntas basada en el estándar ISO 27001 al personal de TI, incluidas las áreas de desarrollo, infraestructura y soporte académico.

De manera similar se realizó una inspección de campo para conocer los activos que posee la institución y el diseño de red que se maneja, a fin de verificar cómo se lleva a cabo la seguridad de la información, así como la protección de los activos pertenecientes a la institución.

3.1.1. MATRIZ DE ENTREVISTA.

En la entrevista realizada al Administrador Jefe tratamos de obtener la información generalizada de cómo está operando el departamento de TI.

A continuación, mostramos la Matriz de la Entrevista realizada con las respuestas obtenidas.

Tabla 1: Matriz de Entrevista

#	Pregunta	Observación
1	¿Tiene algún conocimiento con respecto a la Seguridad de la Información?	Existe una autoeducación. El conocimiento es obtenido a través de documentación alojada en la web.
2	¿Qué grado de conocimiento tiene usted con respecto a la NORMA ISO 27001?	Se entiende que es la forma en cómo se maneja la documentación y los procesos existentes.
3	¿Qué implica para usted el brindar seguridad informática en la institución?	Validar si existen brechas de seguridad sobre la red.
4	¿Se ha ejecutado alguna prueba de Hacking Ético sobre la red interna?	No se ha realizado.
5	¿Los empleados son capaces de identificar un virus/malware?	Sí, inclusive se tiene precaución de no caer en ataques como Phishing.

6	¿Están sus empleados formados en seguridad de la información y gestión de riesgos?	No se tiene la certeza de que los empleados cuenten con el conocimiento.
7	¿Poseen monitoreo de las máquinas que acceden a su red Wi-Fi?	Se cuenta con una controladora en donde se verifican los usuarios que están conectados. Sin embargo, no se realiza un monitoreo constante.
8	¿Existe alguna contingencia ante pérdida de enlace para la red Wi-Fi?	No, solo se cuenta con redundancia a nivel WAN.
9	¿En caso de daño de un Wi-Fi, existe un proceso de recuperación?	Sí, se tiene una garantía vigente para estos escenarios.
10	¿Los usuarios que se encuentran en período de vacaciones o que ya no laboran en la empresa son bloqueados?	Sí, se cuenta con un proceso.
11	¿Las claves creadas para acceder a los Sistemas de la Institución tienen caducidad?	No está seguro sobre el tema.
12	¿Las contraseñas son generadas por la Institución o el usuario?	Se crea una contraseña temporal; posteriormente es cambiada por el usuario.
13	Si la genera el usuario, ¿Tienen alguna validación de que sea Contraseña Segura acorde a las normas ISO?	Sí, existe una validación para que cumpla con las normas establecidas.
14	¿Poseen control de acceso para los usuarios de los Sistemas de la Institución?	No
15	¿En la Institución existen acuerdos documentados de Confidencialidad de la Información?	No existen acuerdos.
16	¿Existe Manual de Políticas de Seguridad de la información?	No
17	¿Existe un mecanismo de protección física contra desastres naturales, ataques provocados por el hombre o accidentes?	Sí, se cuenta con un Data Center Alterno TIER IV.
18	¿Los usuarios pueden extraer información a través de dispositivos externos?	Sí, ya que no existe un control sobre los equipos de trabajo (laptops).

19	¿Se realiza un mantenimiento periódico de los equipos de cómputo de la Institución?	Los mantenimientos son programados, por lo general se ejecutan 2 veces al año.
20	¿Existe un control de devolución de activos al momento que un empleado finaliza su contrato?	Sí, se cuenta con un proceso para la devolución de equipos e inclusive se tiene un inventario.

Fuente: Johanna Fierro y Josué Sánchez

3.1.2. EVALUACIÓN DE LA ENTREVISTA APLICADA.

Con base en la entrevista realizada al Administrador Jefe, se pudo evaluar lo siguiente:

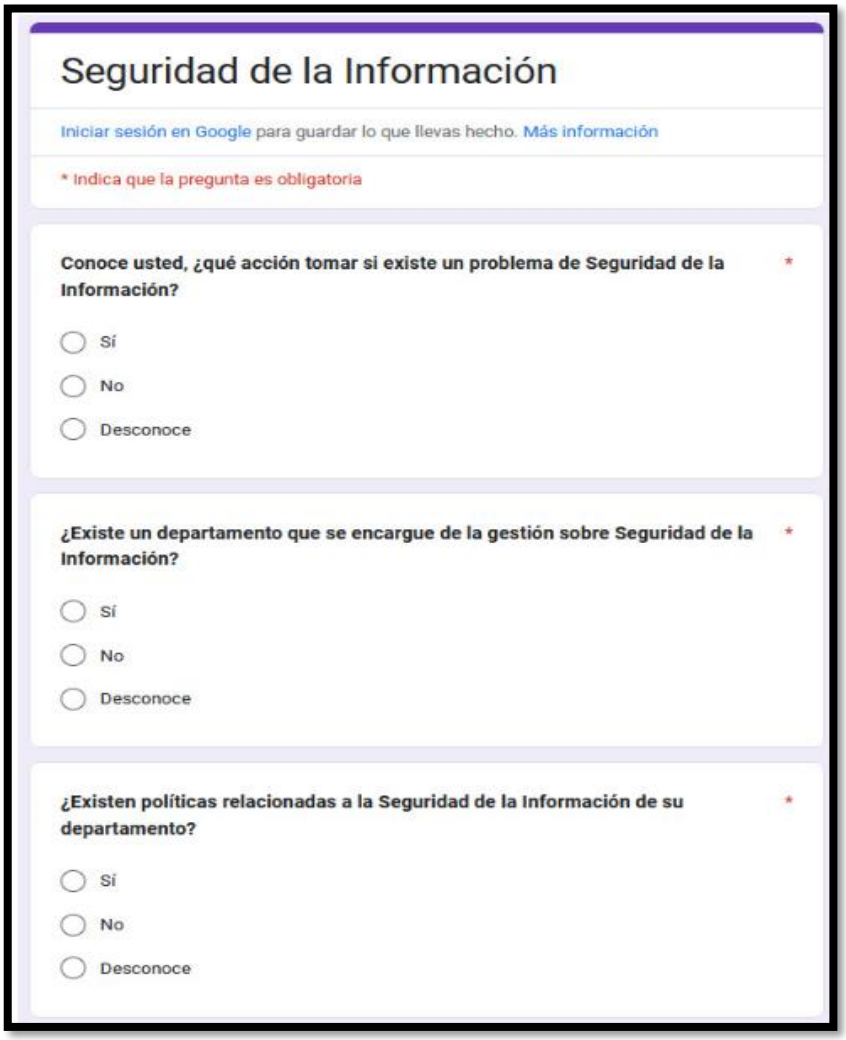
- La Institución no cuenta con un departamento que gestione la Seguridad de la Información y por ende no existen políticas claras ni definidas que guíen al buen tratamiento de los datos.
- Está claro que los empleados tenían pocos conocimientos sobre Seguridad de la Información, y esta falta de conocimiento se debía al hecho de que tienen que autoeducarse.
- Se tiene una idea general de la existencia de la NORMA ISO 27001 y todo lo que comprende. Sin embargo, el Departamento de TI realiza un esfuerzo por tratar de cumplir lo que la norma exige.
- Existe un punto a favor sobre la conexión a la red Wi-Fi, porque mediante la controladora de los APs se pueden monitorear los usuarios finales que se conectan.
- En cuanto a la reposición por daños de un AP, la Institución cuenta con un contrato donde se estipula que el proveedor deberá colocar un nuevo dispositivo.

- Se realiza una buena práctica del uso/creación de contraseñas, como es usar letra mayúscula, mayor a 8 caracteres, que contenga números y hacer uso de caracteres especiales.
- En los dispositivos de computación proporcionados por la Institución, no existe un control de bloqueo sobre los puertos USB y, cualquier empleado puede conectar un dispositivo de almacenamiento de datos y descargar cierta información.
- No se ha realizado una prueba de Hacking Ético sobre la red cableada ni la red Wi-Fi.
- En cuanto a la seguridad física contra desastres naturales, ataques provocados por el hombre o accidentes, la Institución cuenta con un Data Center Alterno mediante el cual se puede brindar la continuidad de sus operaciones.
- Para ciertos equipos de la red, existen mantenimientos preventivos que son programados 2 veces en el año con su proveedor.
- Cuando se presenta la salida de un colaborador, existe un proceso manual en el cual se realiza la devolución de los activos pertenecientes a la Institución. Así mismo, se bloquean los perfiles de usuario creados en su momento.

3.1.3. ENCUESTA

Para complementar la idea sobre el conocimiento sobre Seguridad de la información, realizamos una encuesta al personal del Departamento de TI, con un formulario de 22 preguntas basadas en las políticas de seguridad que nos indica la NORMA ISO 27001.

A continuación, se presentan las preguntas formuladas.



Seguridad de la Información

Iniciar sesión en Google para guardar lo que llevas hecho. Más información

* Indica que la pregunta es obligatoria

Conoce usted, ¿qué acción tomar si existe un problema de Seguridad de la Información? *

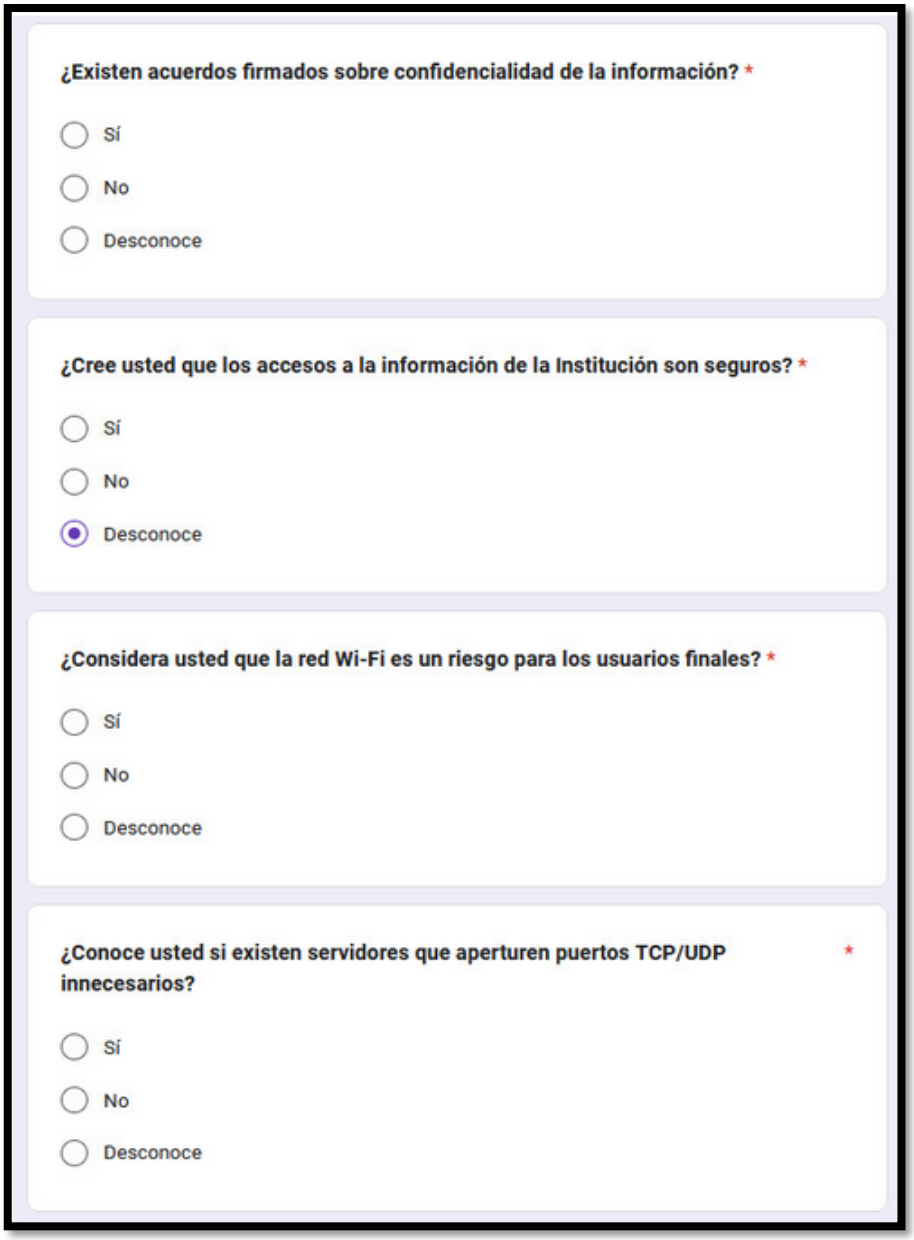
- Sí
- No
- Desconoce

¿Existe un departamento que se encargue de la gestión sobre Seguridad de la Información? *

- Sí
- No
- Desconoce

¿Existen políticas relacionadas a la Seguridad de la Información de su departamento? *

- Sí
- No
- Desconoce



¿Existen acuerdos firmados sobre confidencialidad de la información? *

- ○ Sí
- ○ No
- ○ Desconoce

¿Cree usted que los accesos a la información de la Institución son seguros? *

- ○ Sí
- ○ No
- ◉ Desconoce

¿Considera usted que la red Wi-Fi es un riesgo para los usuarios finales? *

- ○ Sí
- ○ No
- ○ Desconoce

¿Conoce usted si existen servidores que aperturen puertos TCP/UDP innecesarios? *

- ○ Sí
- ○ No
- ○ Desconoce

Las contraseñas que utilizan, ¿poseen una combinación de números, letras y es más de 8 caracteres? *

- ◯ Sí
- ◯ No
- ◯ Desconoce

¿Conoce si se ha ejecutado alguna prueba de Hacking Ético sobre la red interna? *

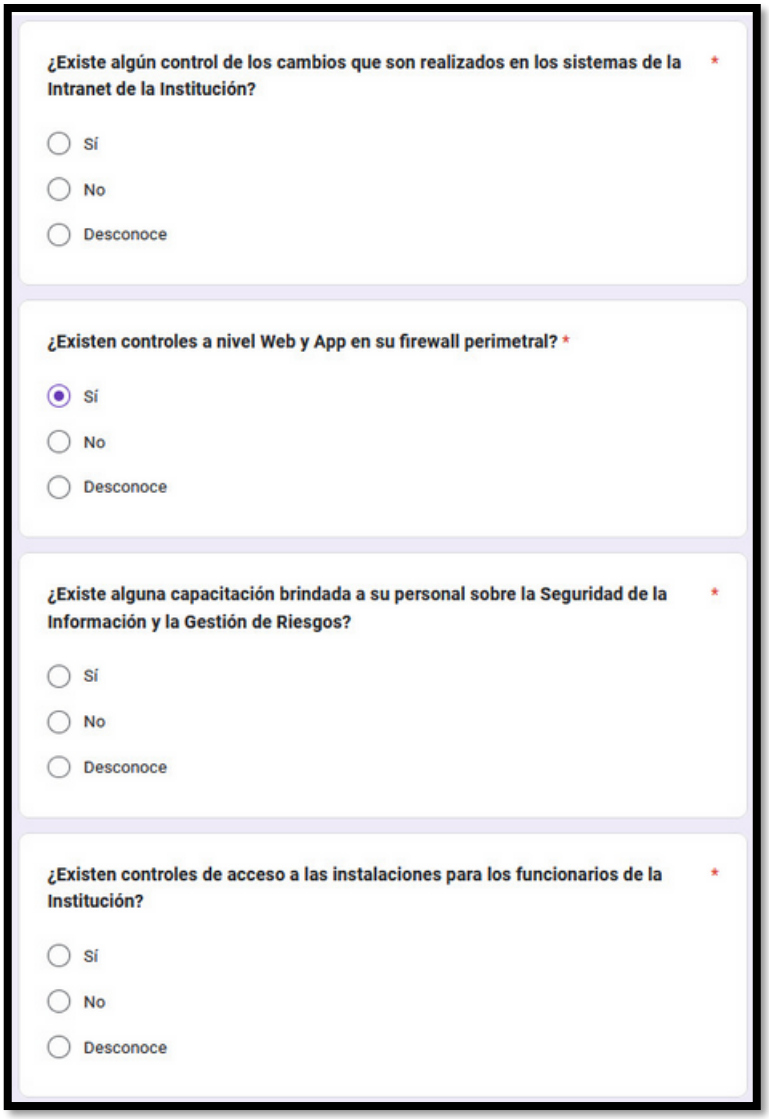
- ◯ Sí
- ◯ No
- ◯ Desconoce

¿Conoce usted si se ha presentado algún tipo de ataque sobre los servicios publicados de la Institución? *

- ◯ Sí
- ◯ No
- ◯ Desconoce

¿Los servidores de la Institución cuentan con sistemas operativos actualizados? *

- ◯ Sí
- ◯ No
- ◯ Desconoce



¿Existe algún control de los cambios que son realizados en los sistemas de la Intranet de la Institución? *

- ○ Sí
- ○ No
- ○ Desconoce

¿Existen controles a nivel Web y App en su firewall perimetral? *

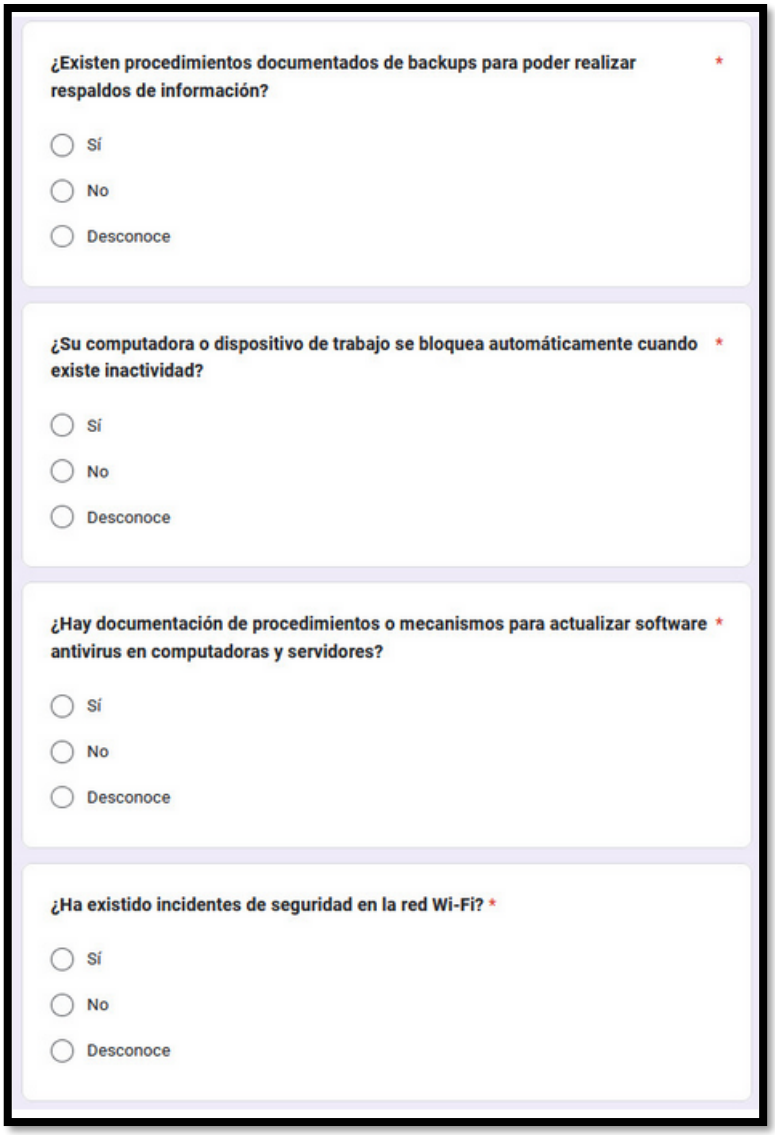
- ◉ Sí
- ○ No
- ○ Desconoce

¿Existe alguna capacitación brindada a su personal sobre la Seguridad de la Información y la Gestión de Riesgos? *

- ○ Sí
- ○ No
- ○ Desconoce

¿Existen controles de acceso a las instalaciones para los funcionarios de la Institución? *

- ○ Sí
- ○ No
- ○ Desconoce



¿Existen procedimientos documentados de backups para poder realizar respaldos de información? *

- Sí
- No
- Desconoce

¿Su computadora o dispositivo de trabajo se bloquea automáticamente cuando existe inactividad? *

- Sí
- No
- Desconoce

¿Hay documentación de procedimientos o mecanismos para actualizar software antivirus en computadoras y servidores? *

- Sí
- No
- Desconoce

¿Ha existido incidentes de seguridad en la red Wi-Fi? *

- Sí
- No
- Desconoce

¿Existe un control de credenciales para los colaboradores que cesan en sus funciones? *

- ◯ Sí
- ◯ No
- ◯ Desconoce

¿Conoce si existen garantías sobre los equipos de telecomunicaciones, sean estos; routers, switches, access points, etc? *

- ◯ Sí
- ◯ No
- ◯ Desconoce

¿Existen mantenimientos periódicos sobre la infraestructura física de la red (cableado estructurado, climatización, UPS, rack, etc)? *

- ◯ Sí
- ◯ No
- ◯ Desconoce

3.1.4. TABULACIÓN DE RESULTADOS

En la encuesta realizada a las 33 personas que comprenden el Departamento de TI, solamente se obtuvieron 25 respuestas y con esta información se analizará más adelante.

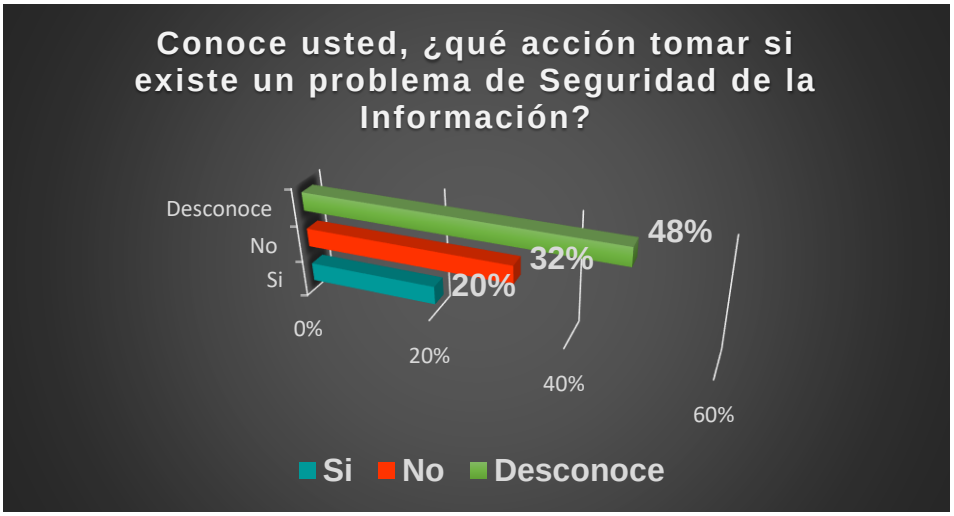


Figura 3.1: Seguridad de la Información
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

.

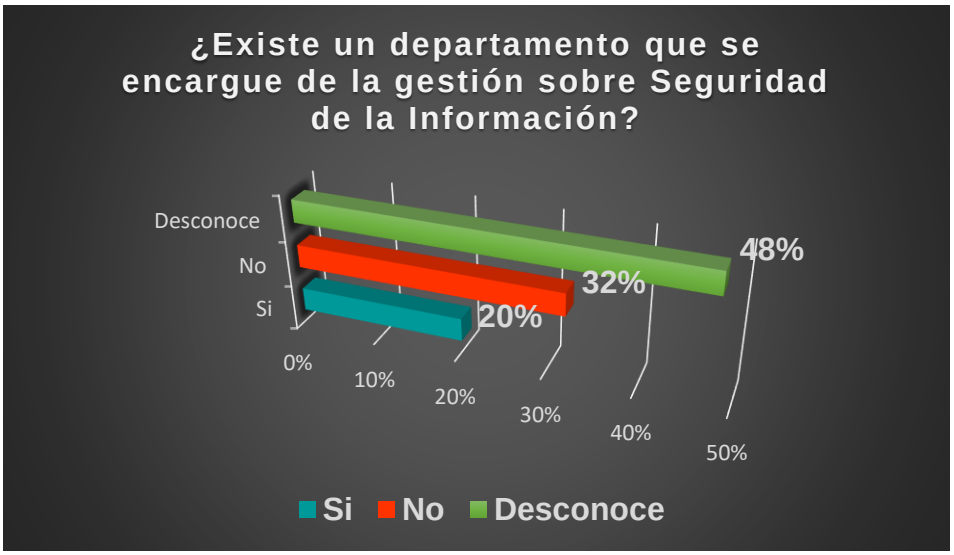


Figura 3.2: Gestión de Seguridad de la Información
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

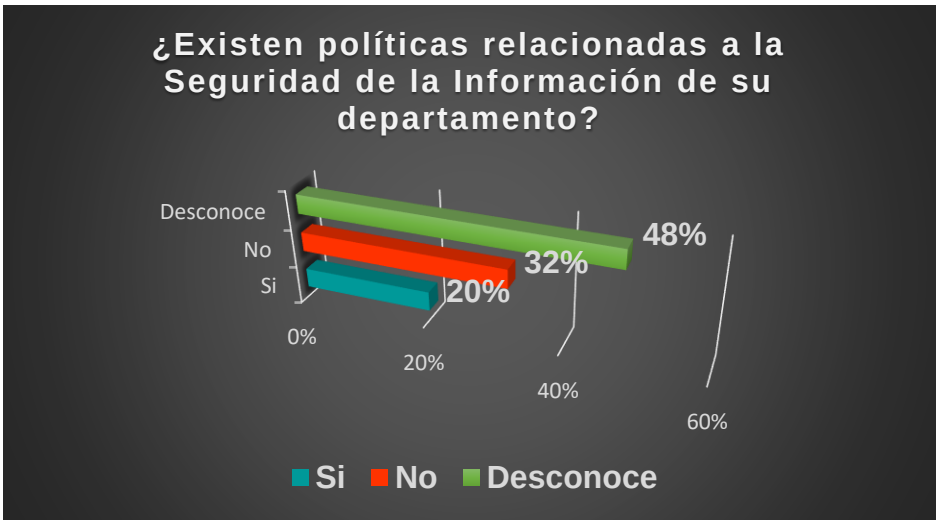


Figura 3.3: Políticas de Seguridad.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

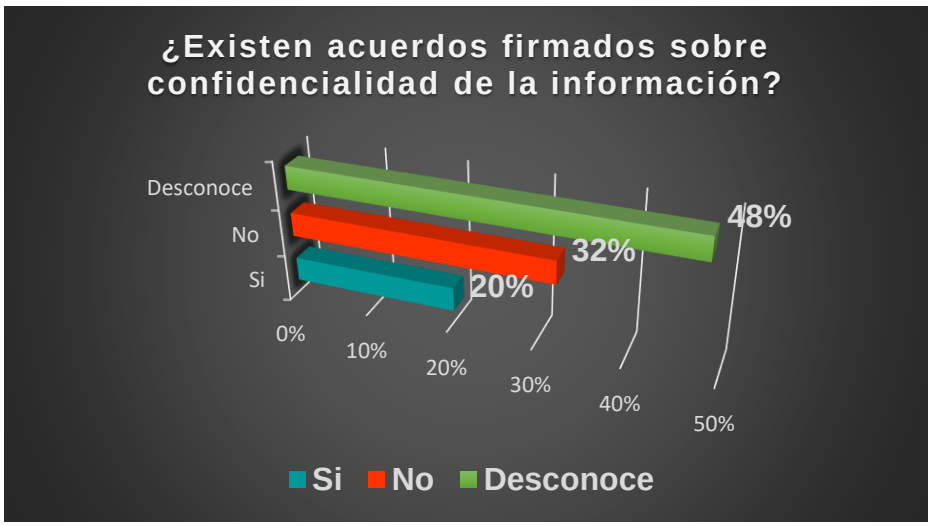


Figura 3.4: Acuerdos de Confidencialidad
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

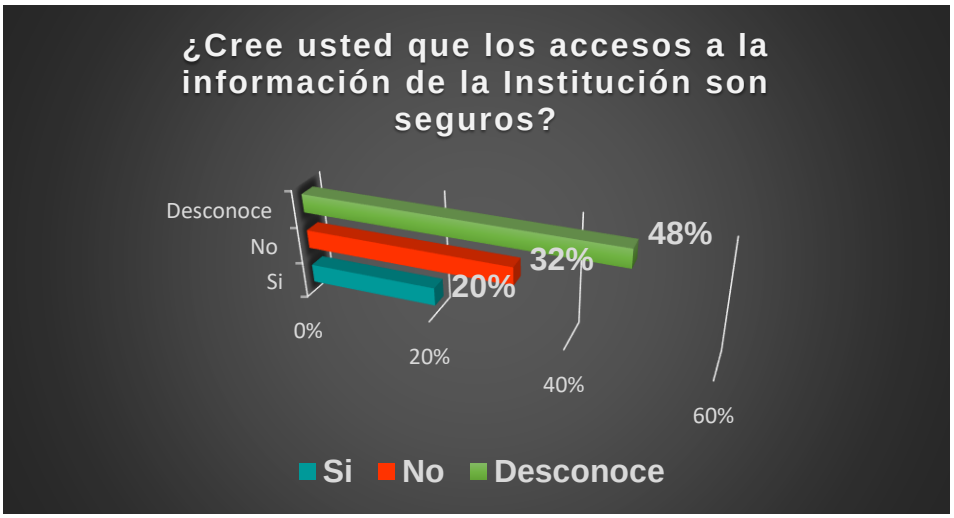


Figura 3.4: Accesos a la Información.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

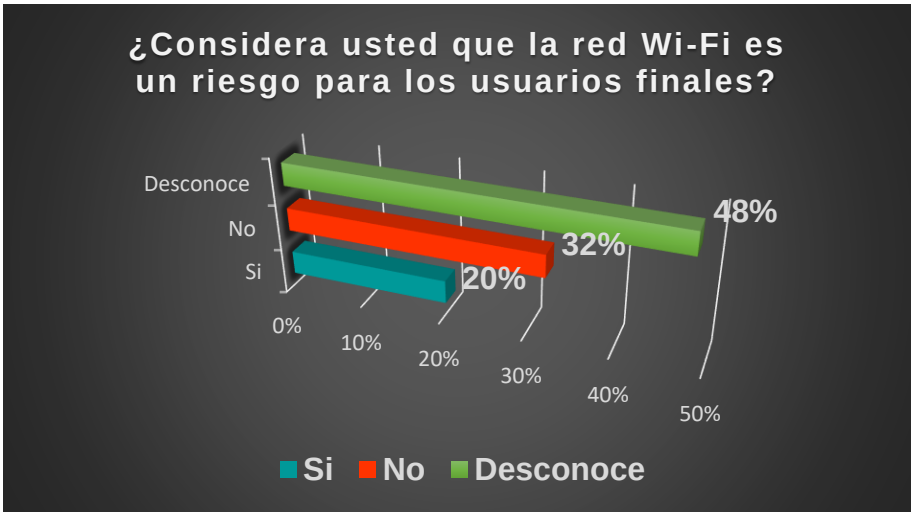


Figura 3.5: Wi-Fi es un riesgo?
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

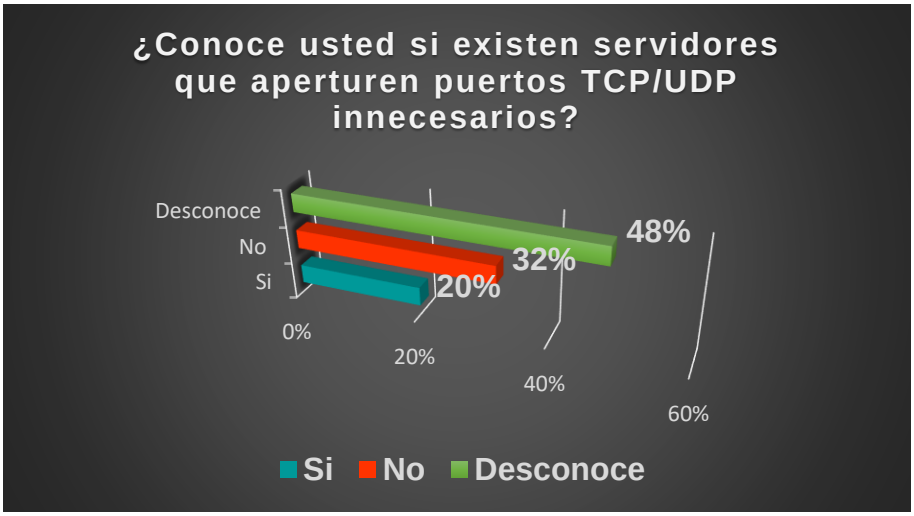


Figura 3.6: Servidores con puertos abiertos innecesariamente.
Fuente: Elaborado por Johanna Fierro y Josué Sánchez.

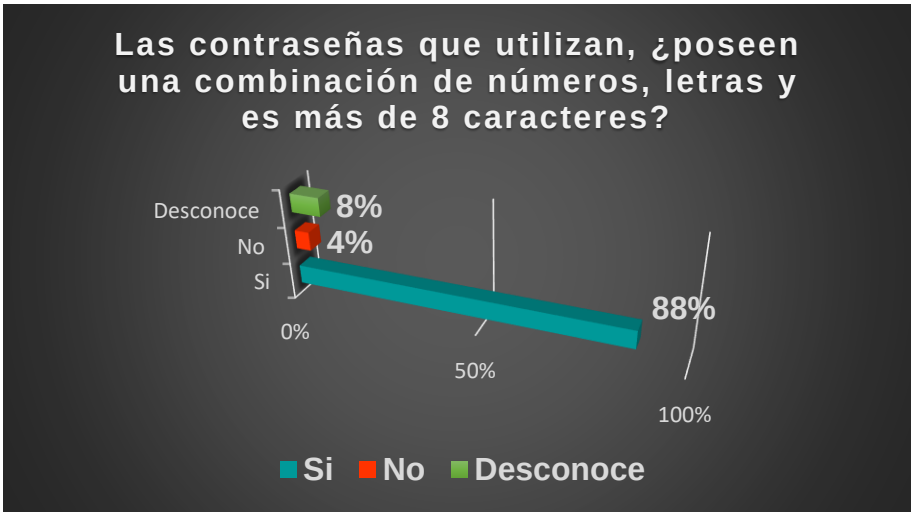


Figura 3.7: Contraseñas
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

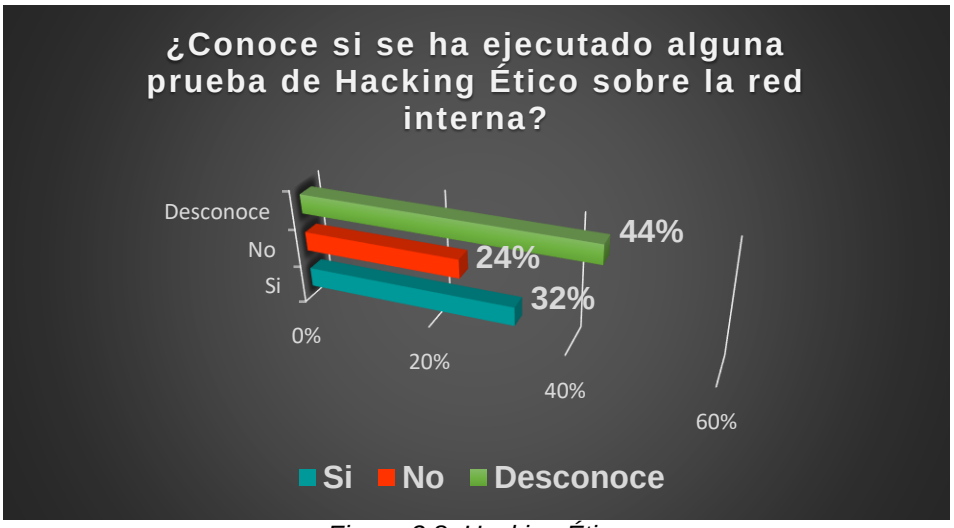


Figura 3.8: Hacking Ético
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

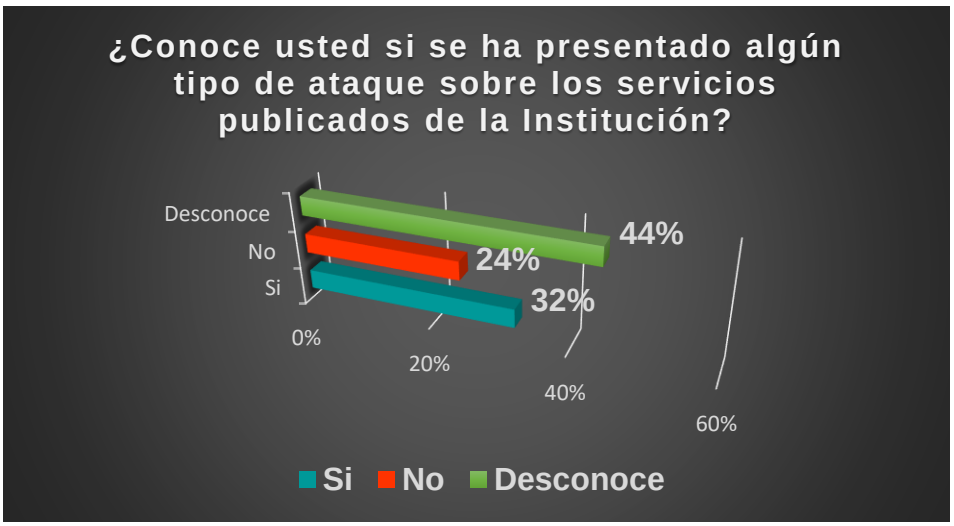


Figura 3.9: Ataques sobre Servicios Publicados
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

Figura 3.10: Servidores Actualizados
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

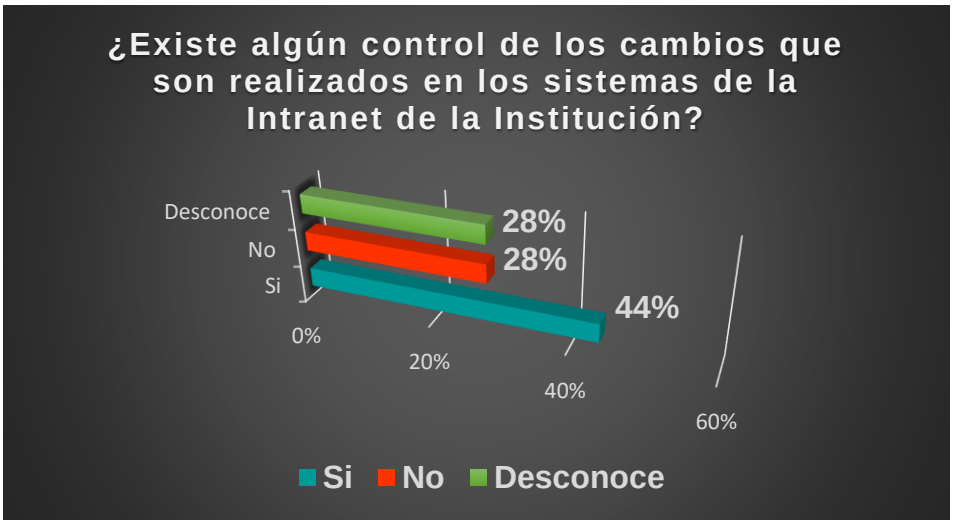


Figura 3.11: Control de Cambios
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

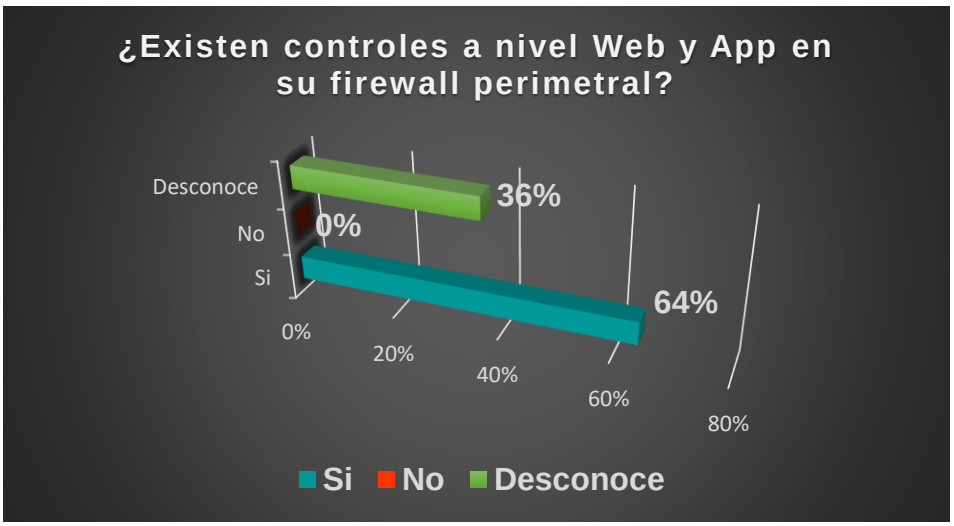


Figura 3.12: Controles en Firewall
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

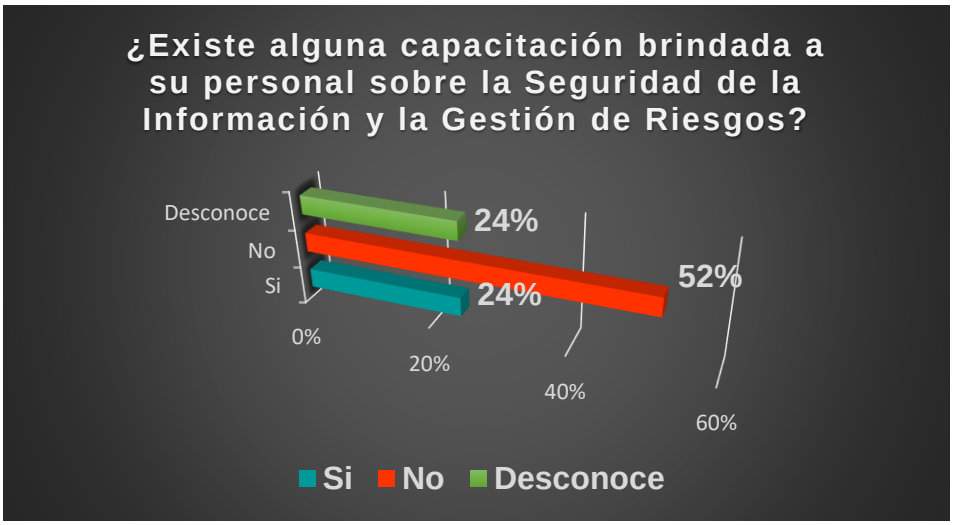


Figura 3.13: Capacitación
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

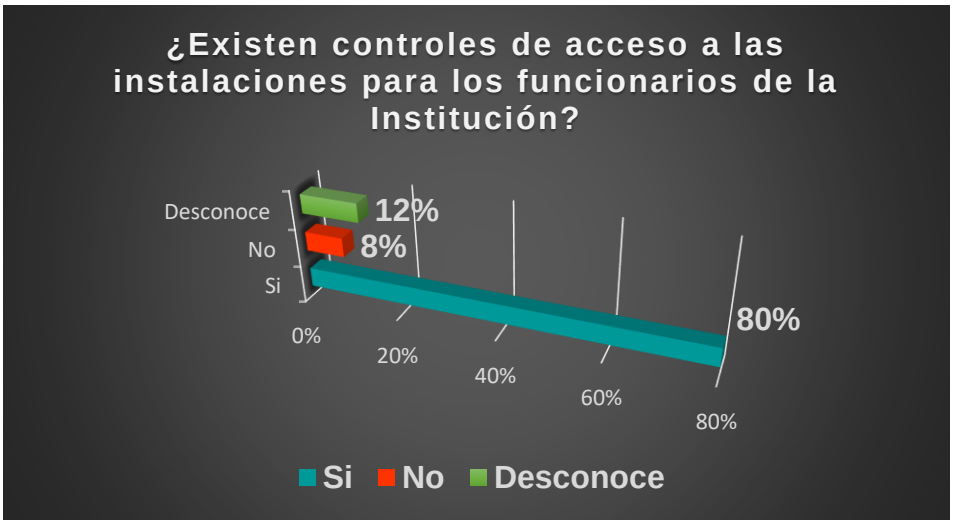


Figura 3.14: Control Acceso a las Instalaciones
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

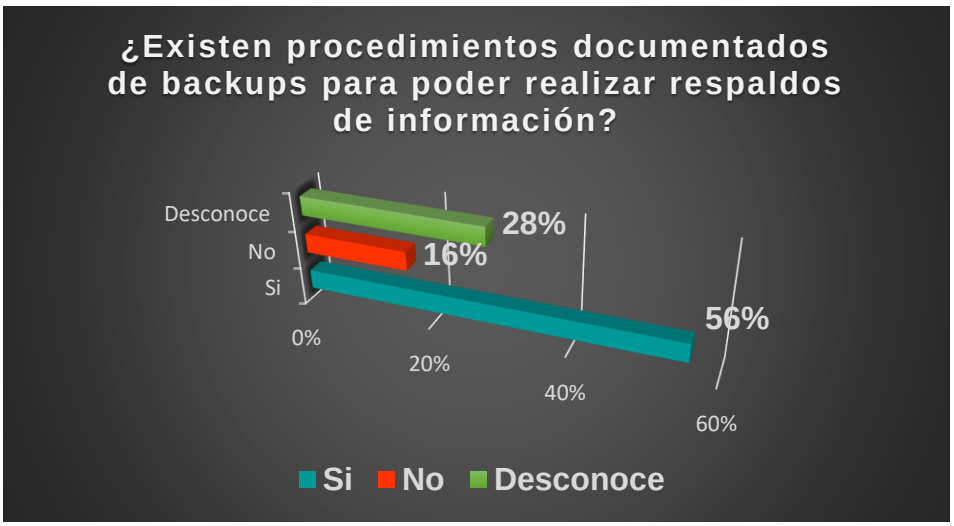


Figura 3.15: Procedimientos Documentados.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

Figura 3.16: Bloqueo de Computadora.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

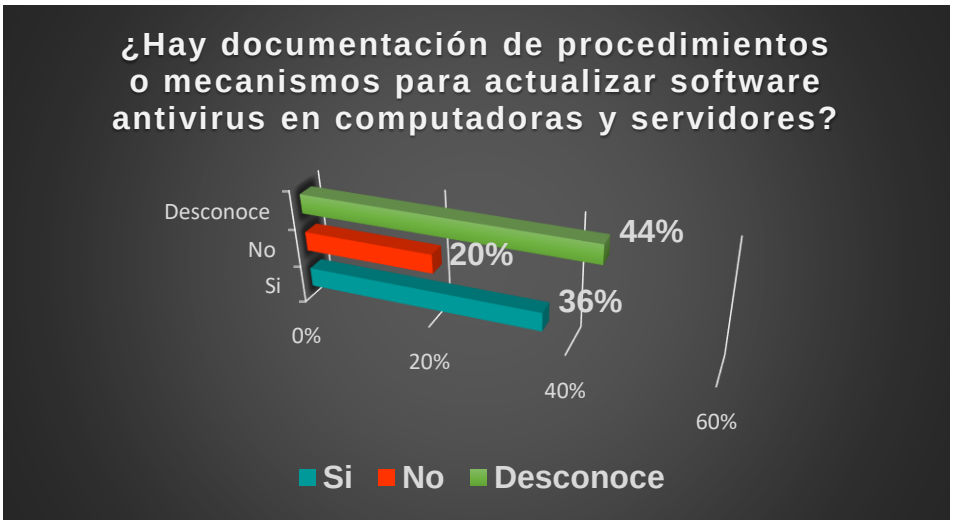


Figura 3.17: Documentación de Procesos de Actualización de Software.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

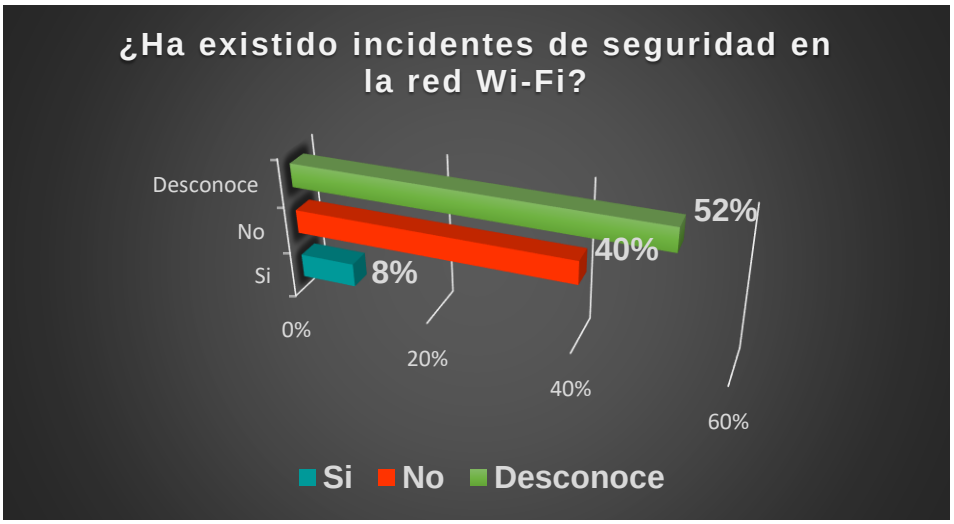


Figura 3.18: Incidentes de Seguridad Red Wifi.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

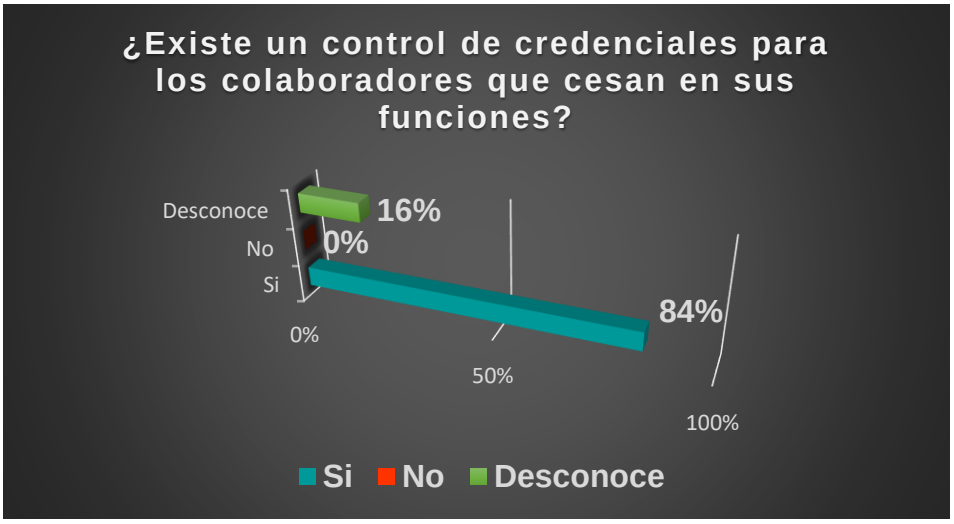


Figura 3.19: Control de Credenciales en Colaboradores cesados.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

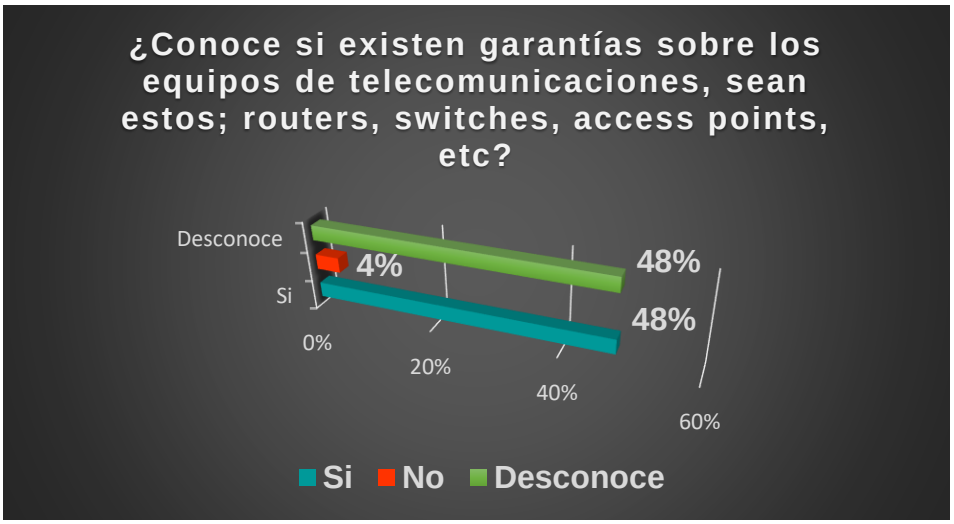


Figura 3.20: Garantías de Equipos.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

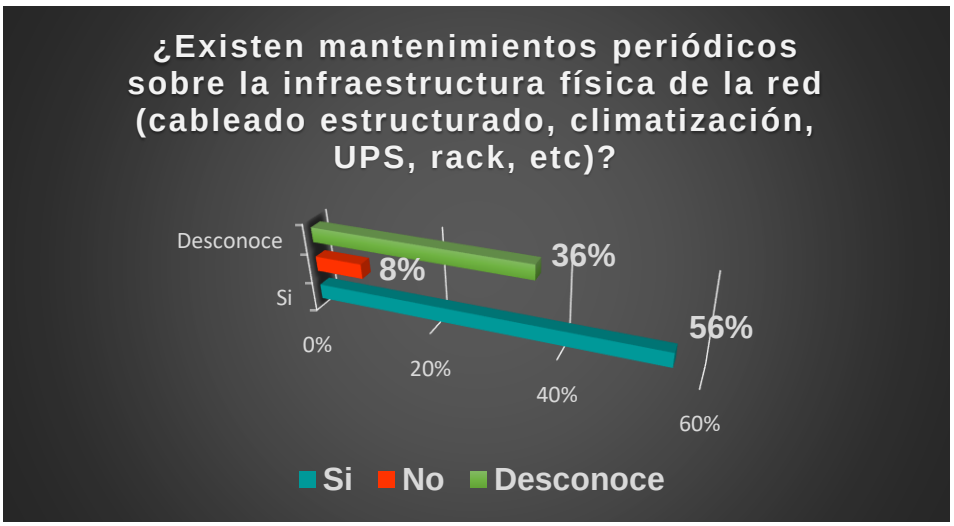


Figura 3.21: Mantenimientos.
Fuente: Elaborada por Johanna Fierro y Josué Sánchez.

3.2. ANÁLISIS DE RESULTADOS

En base a lo expresado en la entrevista y encuesta, y con la tabulación realizada, se logra determinar que:

Los conocimientos sobre Seguridad de la Información son escasos y sin bases sólidas, ya que la respuesta asertiva de menos de un tercio del Departamento TI sobre lo consultado es lo que más se ha repetido en la encuesta.

No existe un Departamento de Seguridad de la Información; carecen de procesos de seguridad definidos, menos aún documentados, sobre los procedimientos para obtener backups solamente conocen un mínimo de personas y el desconocimiento de los compromisos y obligaciones que tienen para proteger la información es más del 60%.

Existen muchos incumplimientos a la Norma que se han reflejado en estas exploraciones a la Jefatura y personal del Departamento de TI.

CAPÍTULO IV

DETERMINACIÓN DE LOS POSIBLES PUNTOS DE ACCESOS VULNERABLES EN LA RED MEDIANTE HACKING ÉTICO.

Nuestro proyecto se basa en el Desarrollo de un Plan de Mejora para la Seguridad de la Información y para poder ejecutarlo eficientemente es necesario determinar cuáles son los puntos vulnerables existentes en la red.

4.1. RECOPILACIÓN DE INFORMACIÓN.

Recopilar información y comprender el sistema objetivo es el primer paso en el hacking ético. El reconocimiento es un conjunto de procesos y técnicas (footprinting, escaneo y enumeración) que se utilizan para detectar y recopilar información de forma encubierta sobre los sistemas objetivo.

4.1.1. RECOPILACIÓN PASIVA DE INFORMACIÓN.

La recopilación pasiva de información, como su propio nombre indica, va a consistir en tratar de obtener todos los datos posibles sobre nuestro objetivo interactuando lo mínimo posible con él. En otras palabras, consiste en la recolección de información sobre un objetivo determinado sin que las actividades realizadas por el analista sean mínimamente detectadas por dicho objetivo.

Debemos tener en cuenta que en esta etapa solo accederemos a la información almacenada de manera pública, no intercambiaremos tráfico de red con el objetivo ni realizaremos peticiones a las aplicaciones web ni ningún sistema que esté expuesto.

Hacking con Buscadores

Todos los buscadores nos brindan funciones avanzadas, comandos y operaciones booleanas con las que podemos crear consultas más complejas de las que solemos hacer y que nos permiten encontrar información muy específica que se encuentra publicada en Internet y que estos navegadores han indexado.

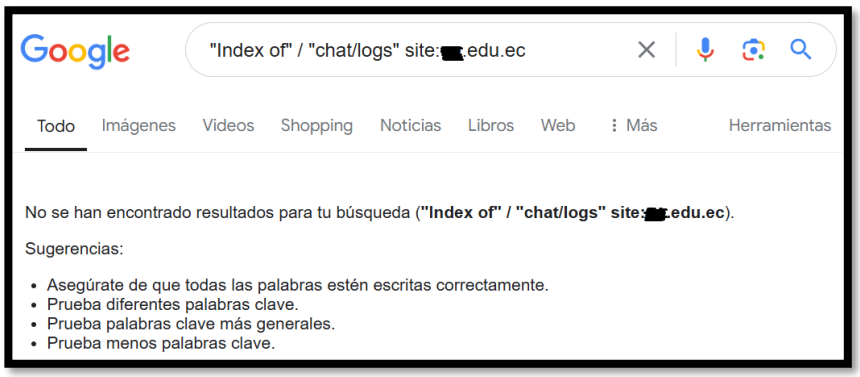


Figura 4.1: Google Dorks Ficheros de Chats
Fuente: Elaborado por Johanna Fierro y Josué Sánchez.

Figura 4.2: Google Dorks Fichero SQL.
Fuente: Elaborado por Johanna Fierro y Josué Sánchez.

Shodan

Es una herramienta de búsqueda en Internet que se centra en la detección de dispositivos y sistemas conectados en la red, como servidores, cámaras de seguridad, routers, bases de datos, entre otros.

Shodan permite buscar dispositivos específicos, explorar vulnerabilidades y obtener información detallada sobre los sistemas conectados. Los resultados de búsqueda pueden incluir información como:

- Direcciones IP
- Puertos abiertos
- Servicios en ejecución
- Versiones de software
- Ubicación geográfica

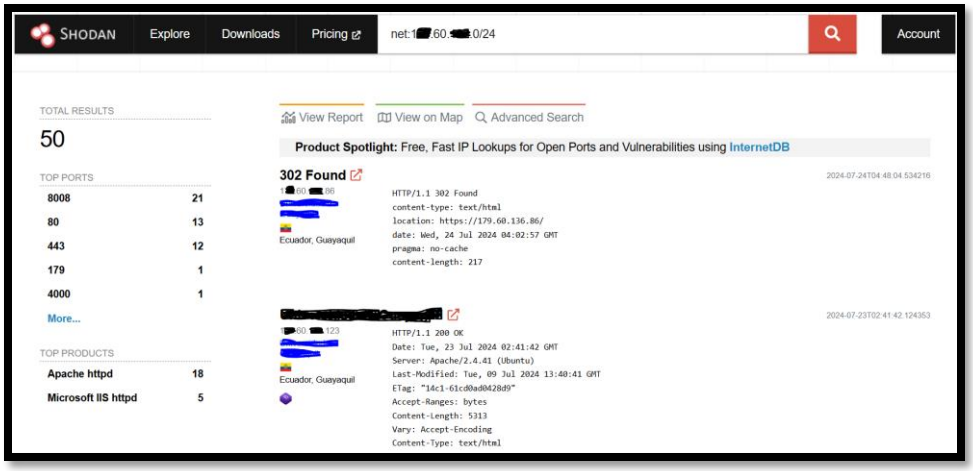


Figura 4.3: Escaneo de puertos con Shodan (Hosts: 86 y 123)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

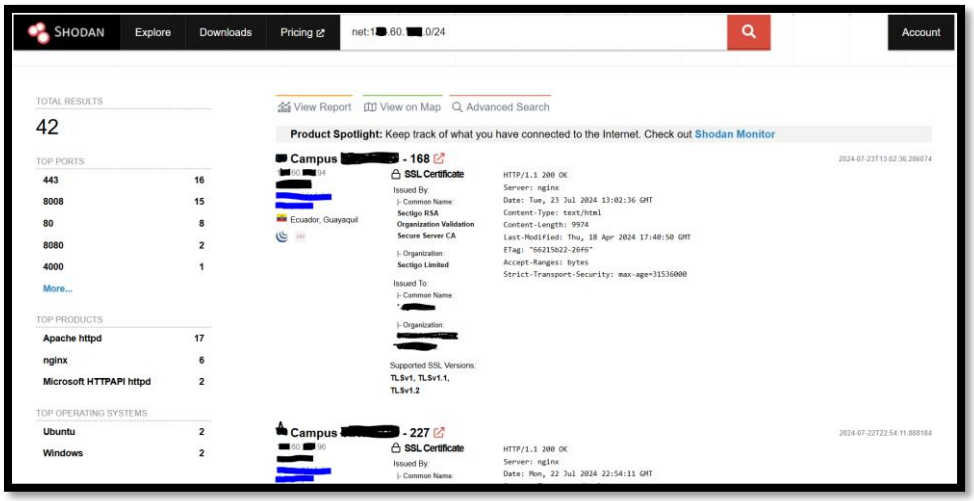


Figura 4.4: Escaneo de puertos con Shodan (Hosts: 94 y 96)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Archive.org (Wayback Machine)

La Wayback Machine es una función de archive.org que permite ver versiones anteriores de sitios web, incluso si han sido eliminados o modificados. Funciona como una máquina del tiempo para el contenido web.

Con la Wayback Machine, podremos:

- Ver versiones antiguas de sitios web
- Recuperar contenido eliminado

- Ver cómo ha cambiado un sitio web con el tiempo.
- Acceder a sitios web bloqueados o inaccesibles.

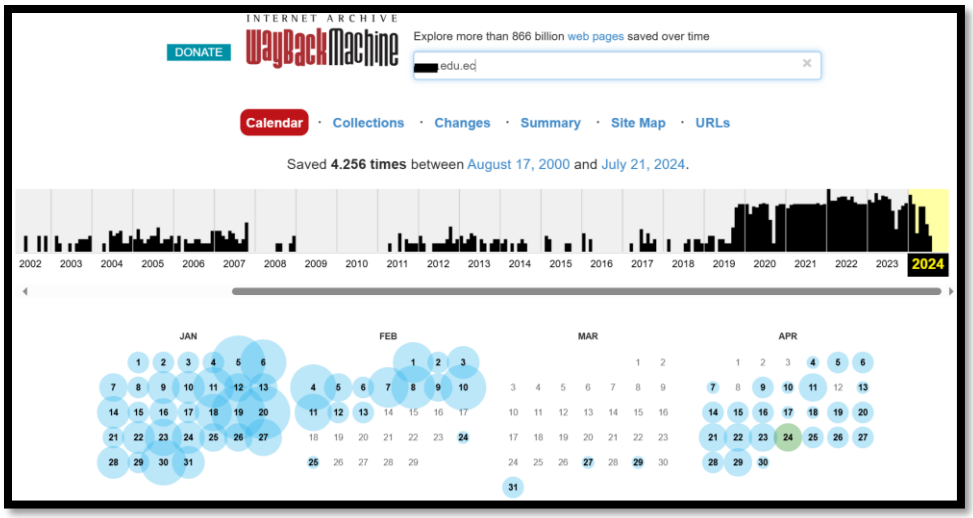


Figura 4.5: Verificación en el tiempo de la página web
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

4.1.2. RECOPILACIÓN SEMI-PASIVA DE INFORMACIÓN

A diferencia de la etapa anterior, en la que no se intercambiaba tráfico de red con el objetivo, en esta fase usaremos métodos que interactuarán con nuestro objetivo, teniendo en cuenta que nuestro objetivo no se dará cuenta de que ese tráfico de red proviene de la recopilación de información. Por lo tanto, en esta fase, recopilaremos información sobre un objetivo determinado utilizando métodos que se asimilen al tráfico de red y comportamiento normal que suele recibir.

Dentro del alcance se encuentran actividades como:

- Consultas a servidores DNS
- Acceso a recursos internos de las aplicaciones web
- Análisis de metadatos de documentos.

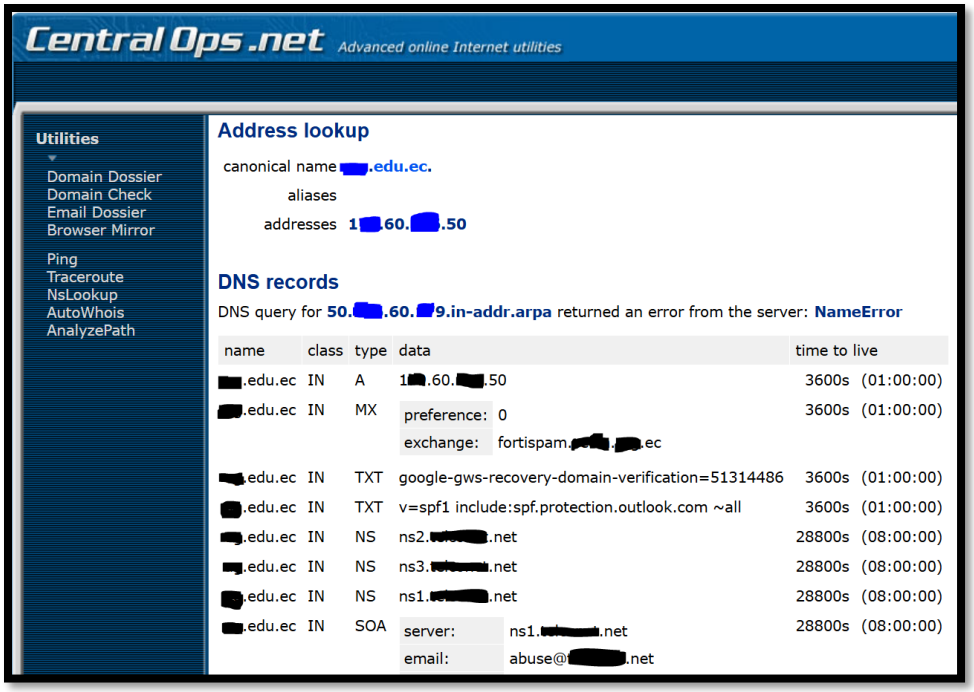


Figura 4.6: Registros DNS con Central OPS
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Figura 4.7: Registros con DNS Dumpster GeoIP Location
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Figura 4.8: Registros A con DNS Dumpster
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

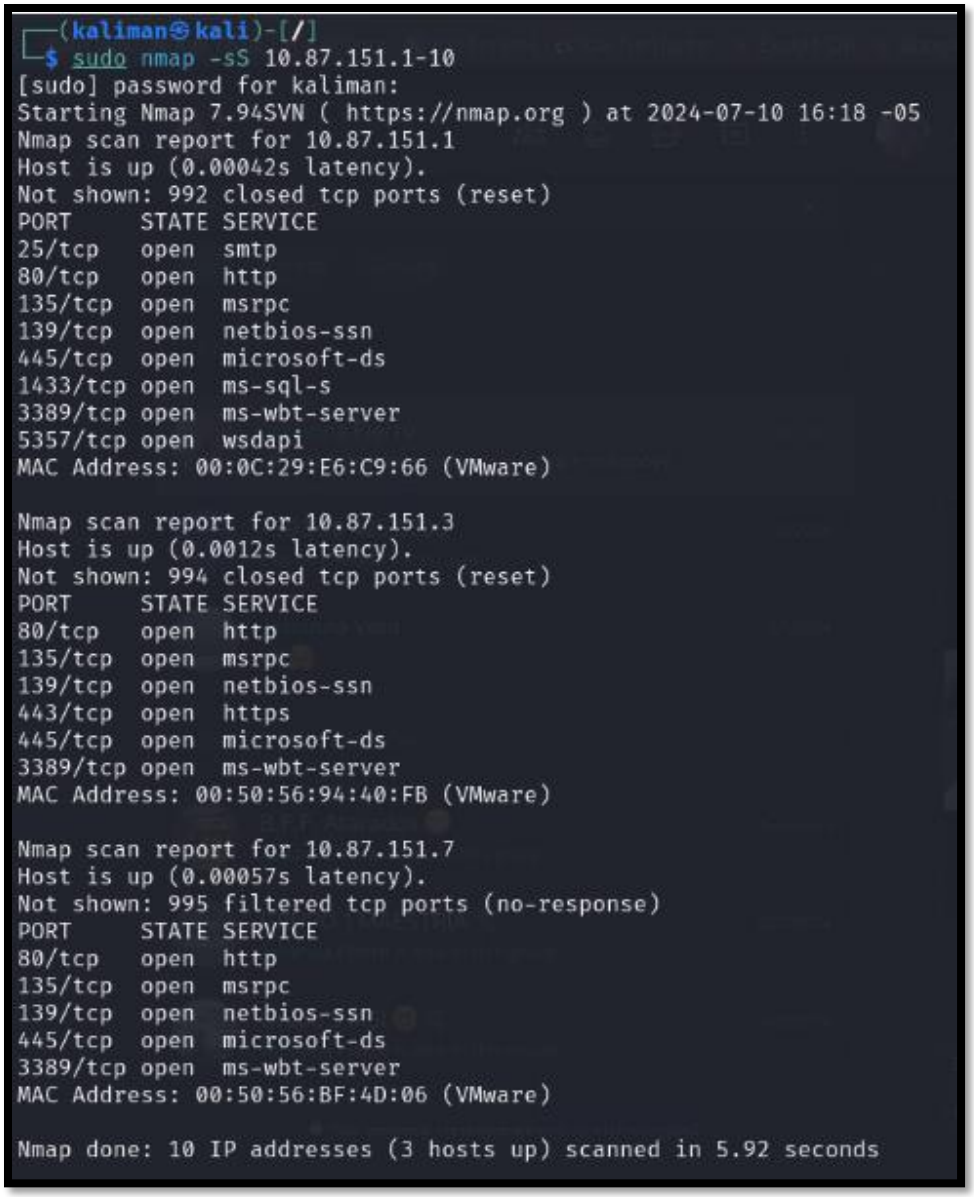
4.1.3. RECOPILACIÓN ACTIVA DE INFORMACIÓN

Esta fase tiene como objetivo recolectar información sobre un objetivo determinado utilizando métodos que interactúan de manera directa con el objetivo, normalmente mediante el envío de tráfico de red.

En esta fase, utilizaremos herramientas y técnicas que van a establecer conexiones específicas con nuestro objetivo para tratar de obtener una serie de datos, una serie de intuiciones que nos sirvan a nosotros para continuar con nuestro ejercicio Hacking Ético. Es importante destacar que todas estas técnicas son invasivas y pueden ser detectadas como actividad sospechosa o maliciosa por herramientas como un WAF, un firewall, un sistema de detección de intrusiones (IDS) e IPS.

Dentro del alcance se encuentran actividades como:

- Escáneres de hosts
- Escáneres de puertos
- Escáneres de servicios



```
┌──(kaliman㉿kali)-[/]
└─$ sudo nmap -sS 10.87.151.1-10
[sudo] password for kaliman:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 16:18 -05
Nmap scan report for 10.87.151.1
Host is up (0.00042s latency).
Not shown: 992 closed tcp ports (reset)
PORT     STATE SERVICE
25/tcp   open  smtp
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:0C:29:E6:C9:66 (VMware)

Nmap scan report for 10.87.151.3
Host is up (0.0012s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:94:40:FB (VMware)

Nmap scan report for 10.87.151.7
Host is up (0.00057s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:BF:4D:06 (VMware)

Nmap done: 10 IP addresses (3 hosts up) scanned in 5.92 seconds
```

Figura 4.9: Escaneo de puertos con NMAP (Hosts: 1 al 10)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

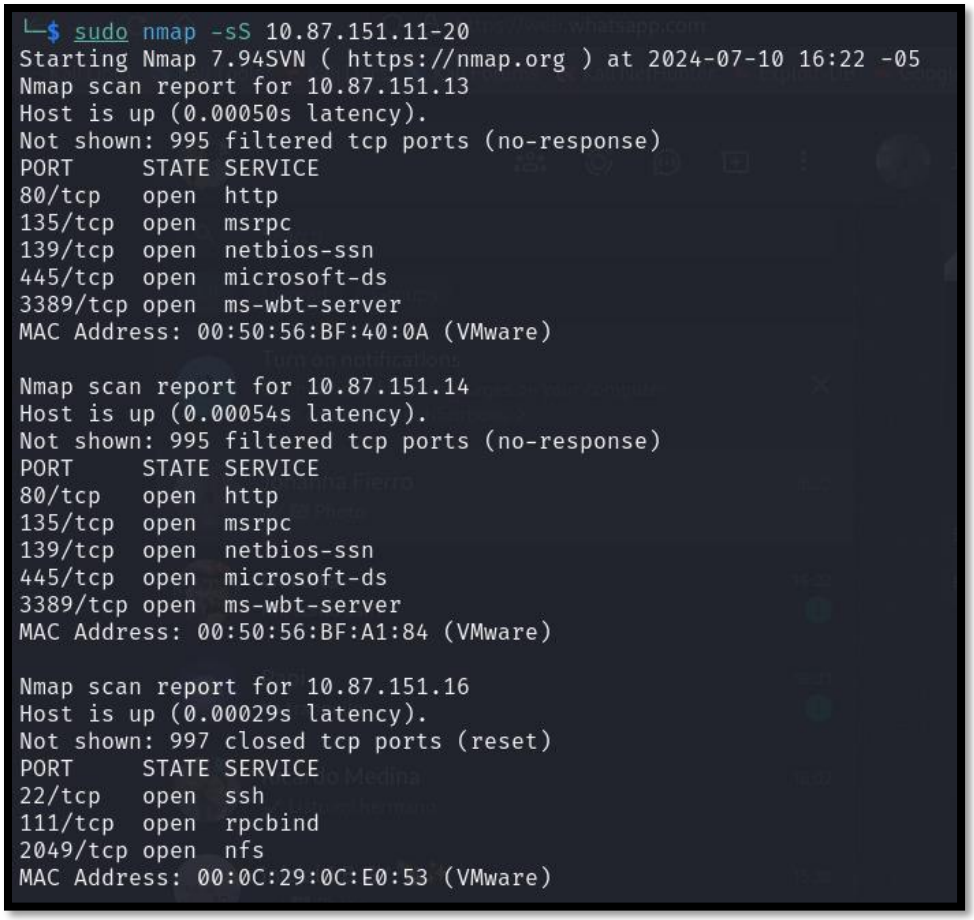


Figura 4.10: Escaneo de puertos con NMAP (Hosts: 13, 14 y 16)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

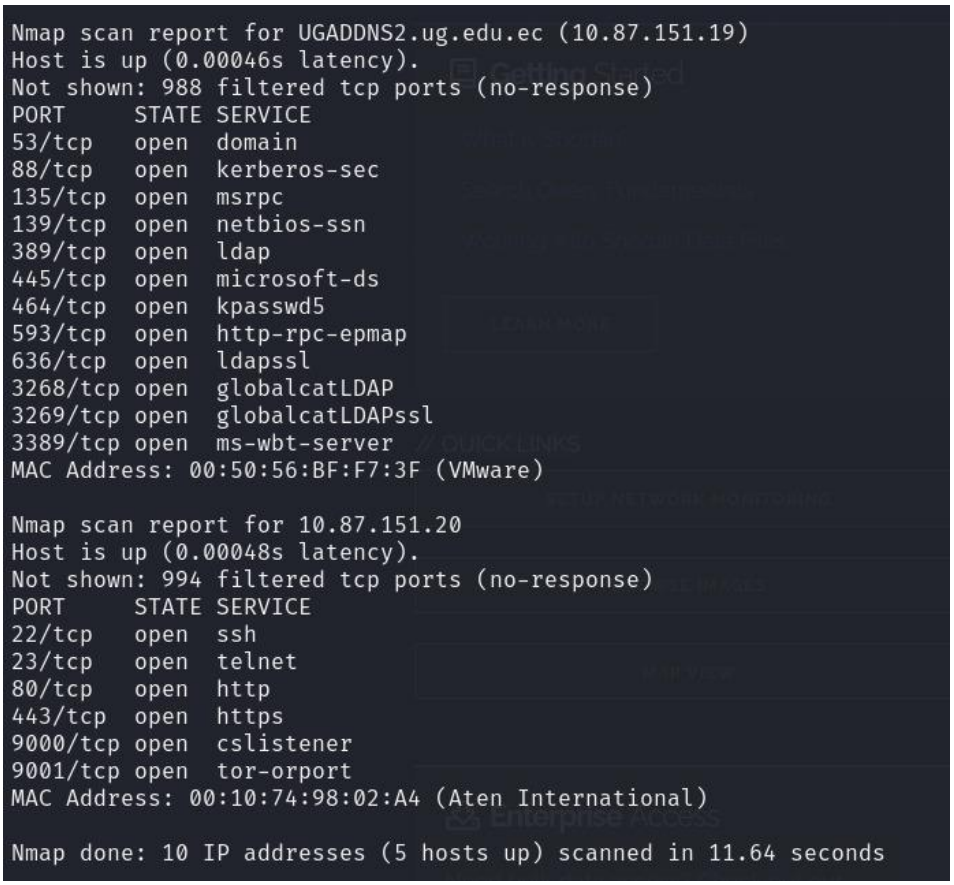


Figura 4.11: Escaneo de puertos con NMAP (Hosts: 19 y 20)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Figura 4.12: Escaneo de puertos con NMAP (Hosts: 21 - 30)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

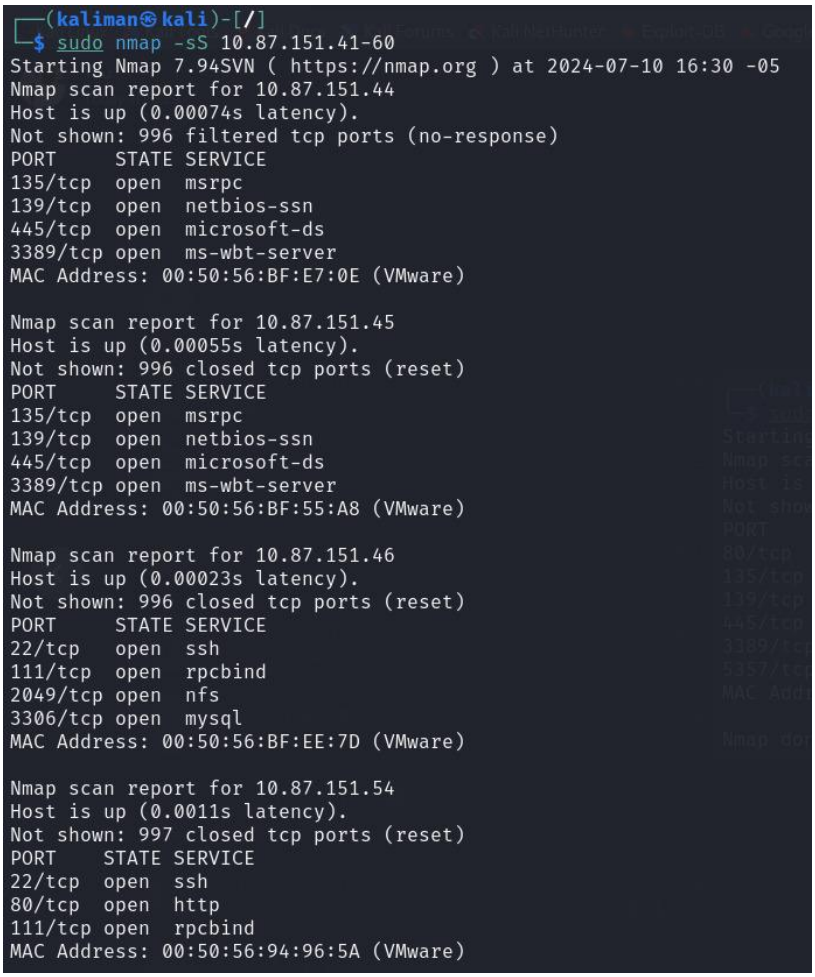
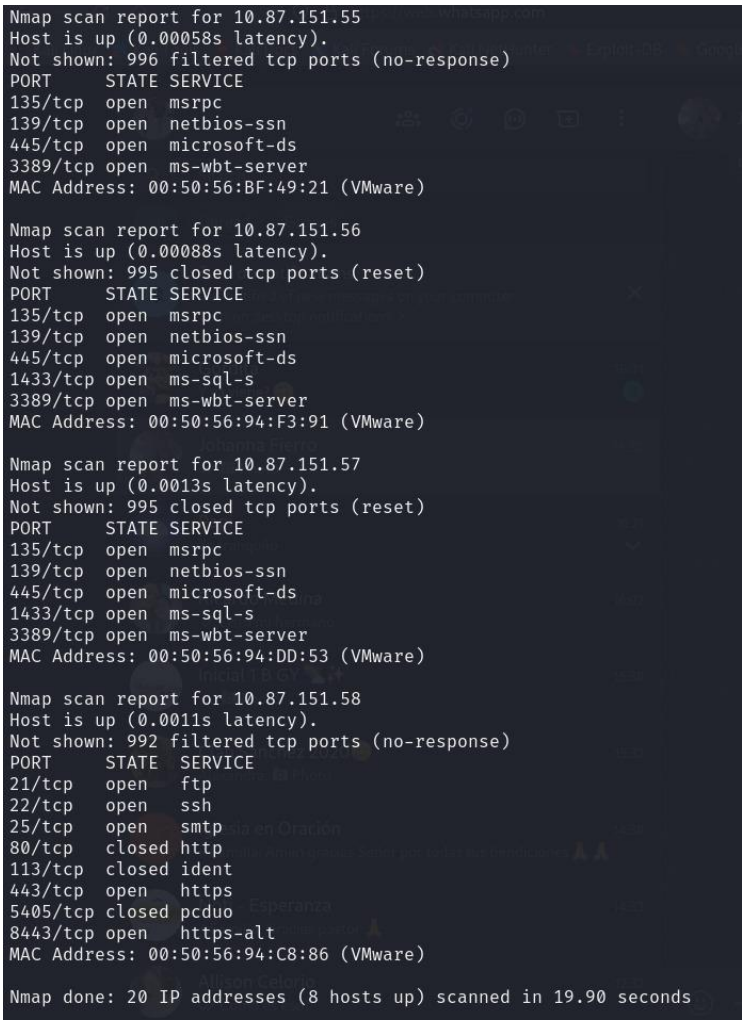
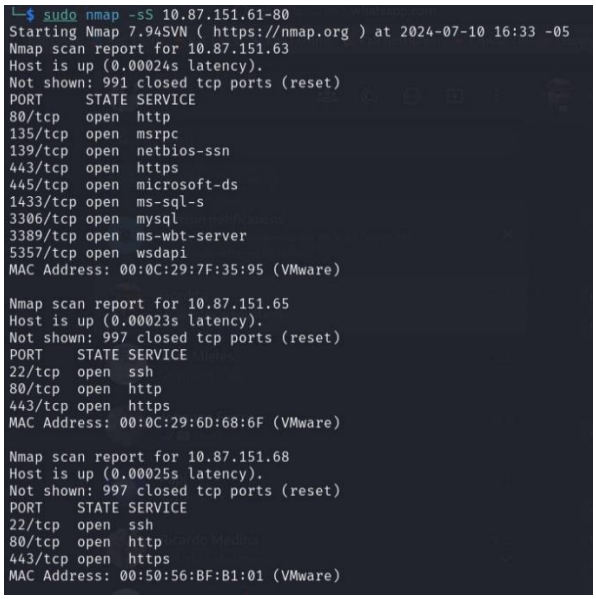


Figura 4.13: Escaneo de puertos con NMAP (Hosts: 44, 45, 46 y 54)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez



```
Nmap scan report for 10.87.151.55
Host is up (0.00058s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:BF:49:21 (VMware)

Nmap scan report for 10.87.151.56
Host is up (0.00088s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:94:F3:91 (VMware)

Nmap scan report for 10.87.151.57
Host is up (0.0013s latency).
Not shown: 995 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:94:DD:53 (VMware)

Nmap scan report for 10.87.151.58
Host is up (0.0011s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
25/tcp   open   smtp
80/tcp   closed http
113/tcp  closed ident
443/tcp  open   https
5405/tcp closed pcduo
8443/tcp open   https-alt
MAC Address: 00:50:56:94:C8:86 (VMware)

Nmap done: 20 IP addresses (8 hosts up) scanned in 19.90 seconds
```

Figura 4.14: Escaneo de puertos con NMAP (Hosts: 55 - 58)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez



```
└─$ sudo nmap -sS 10.87.151.61-80
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 16:33 -05
Nmap scan report for 10.87.151.63
Host is up (0.00024s latency).
Not shown: 991 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
MAC Address: 00:0C:29:7F:35:95 (VMware)

Nmap scan report for 10.87.151.65
Host is up (0.00023s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:0C:29:6D:68:6F (VMware)

Nmap scan report for 10.87.151.68
Host is up (0.00025s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
443/tcp open  https
MAC Address: 00:50:56:BF:B1:01 (VMware)
```

Figura 4.15: Escaneo de puertos con NMAP (Hosts: 63, 65 y 68)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

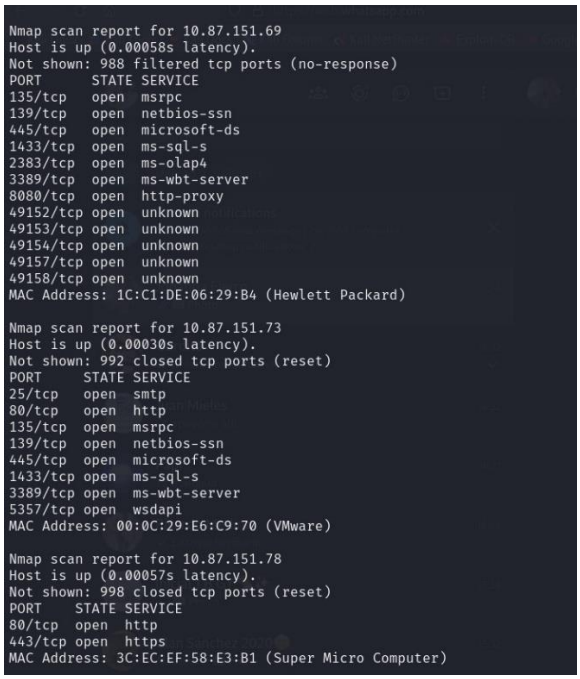


Figura 4.16: Escaneo de puertos con NMAP (Hosts: 69, 73 y 78)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Figura 4.17: Escaneo de puertos con NMAP (Hosts: 79 y 80)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

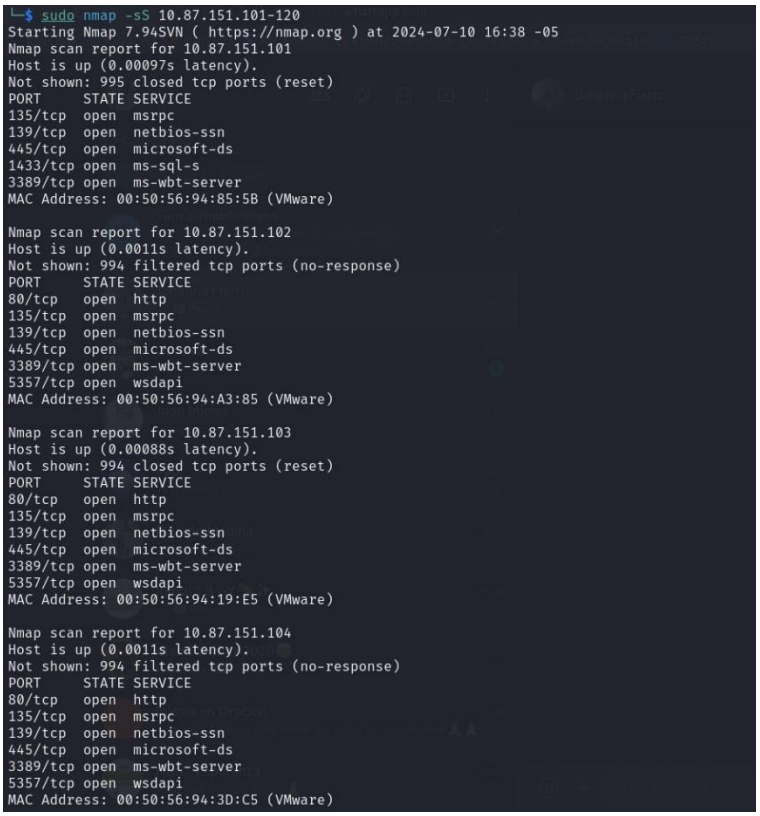


Figura 4.18: Escaneo de puertos con NMAP (Hosts: 101 – 104)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

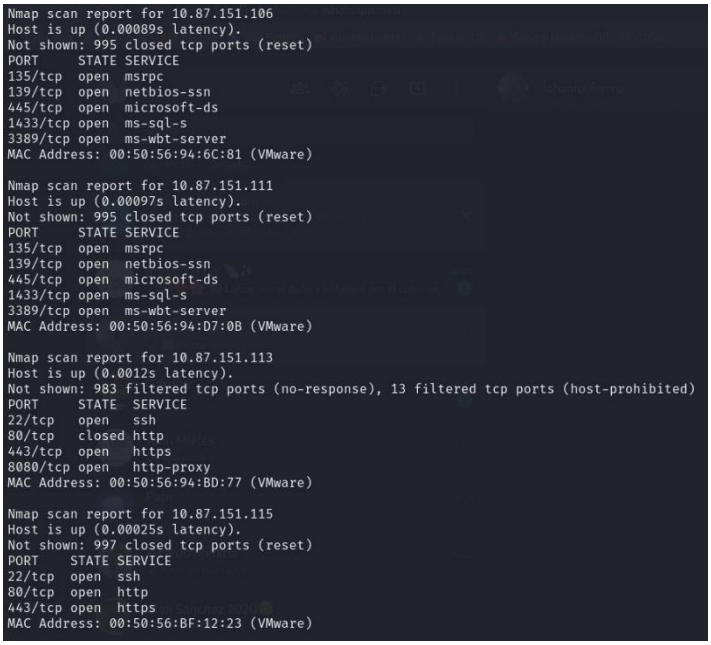


Figura 4.19: Escaneo de puertos con NMAP (Hosts: 106, 111, 113 Y 115)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

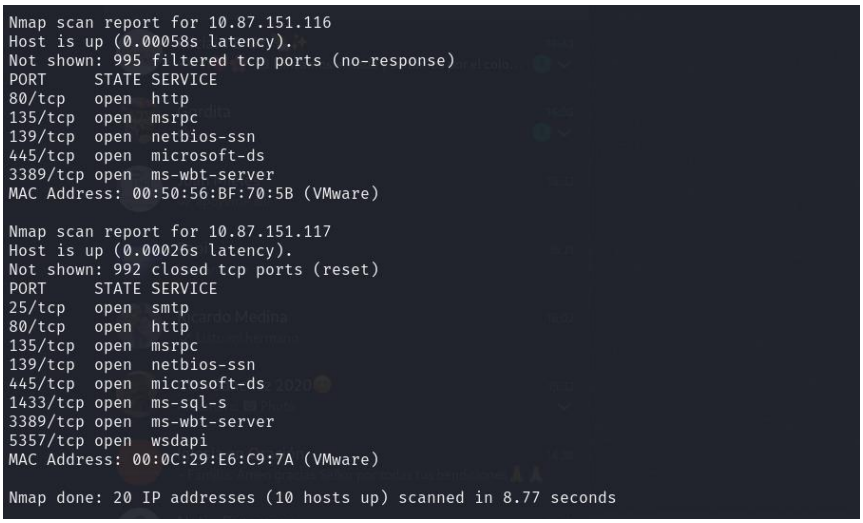


Figura 4.20: Escaneo de puertos con NMAP (Hosts: 116 Y 117)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

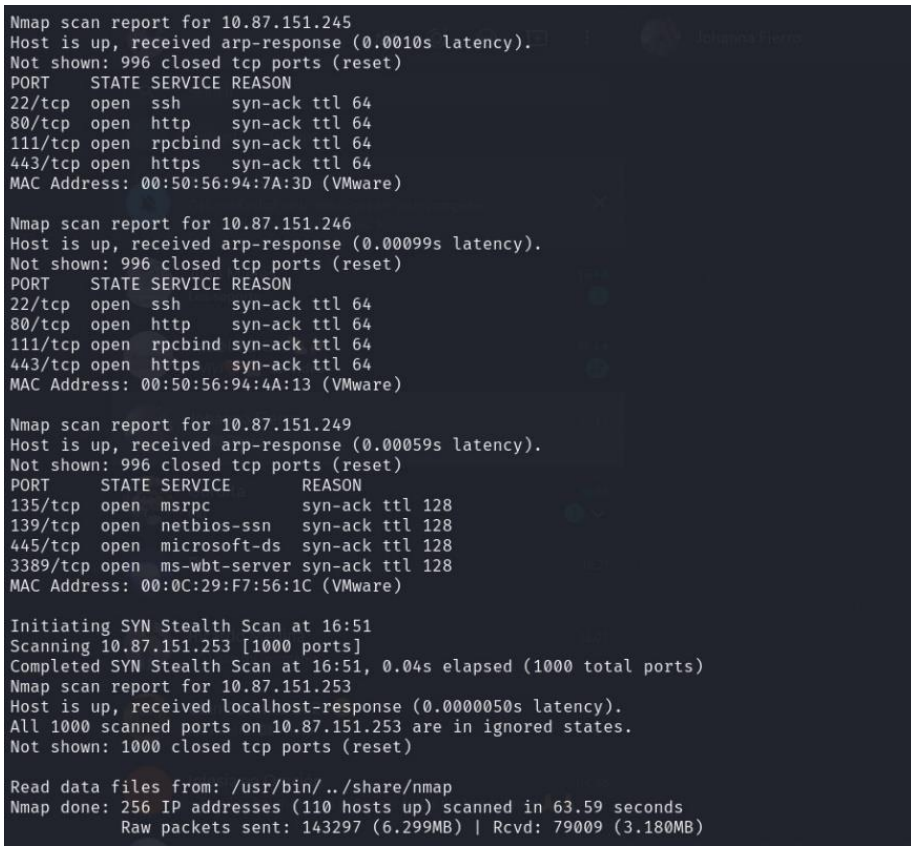


Figura 4.21: Escaneo de puertos con NMAP (Hosts: 245, 246 Y 249)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Las figuras desde la 4.9 a la 4.21 muestran una selección de hosts que están activos en la red y tienen sus puertos abiertos. No obstante, es importante tener en cuenta que no siempre las aplicaciones o servicios estarán disponibles en estos puertos.

Nmap: Descubrimiento de servicios

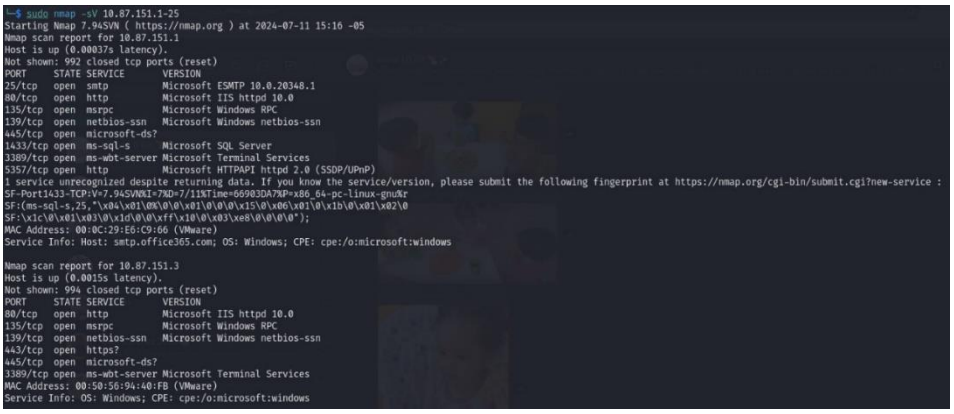


Figura 4.22: Escaneo de Servicios con NMAP (Hosts: 1 y 3)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

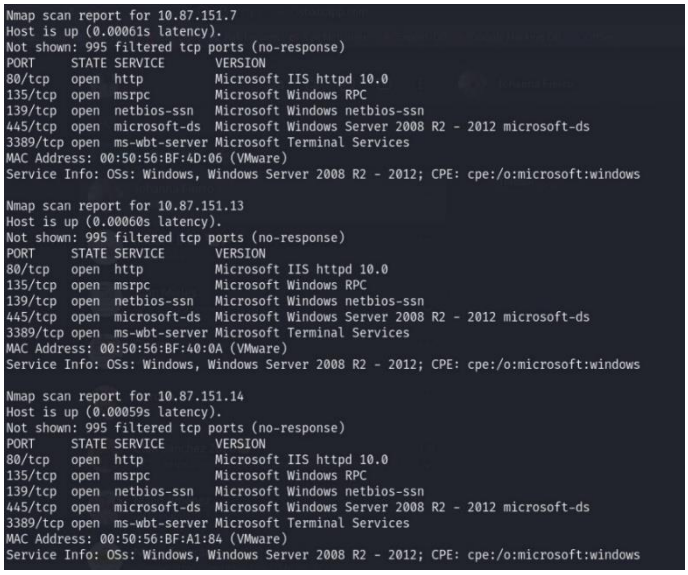


Figura 4.23: Escaneo de Servicios con NMAP (Hosts: 7, 13 y 14)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

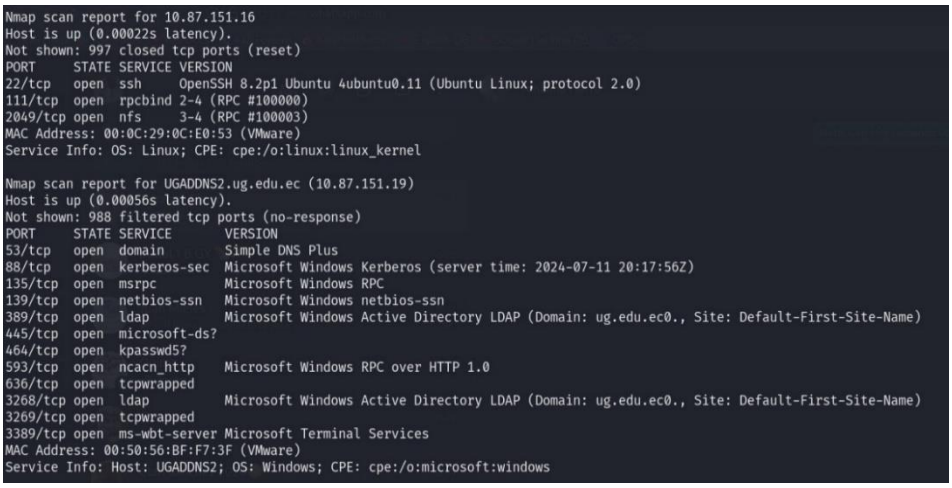


Figura 4.24: Escaneo de Servicios con NMAP (Hosts: 16 y 19)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

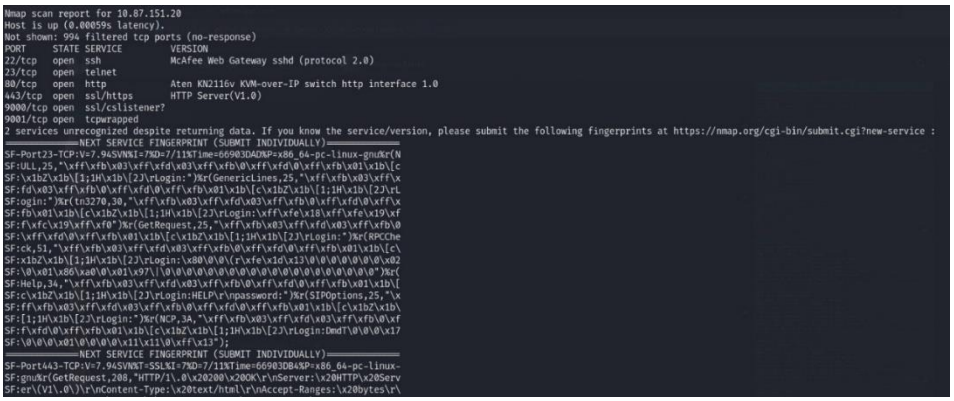


Figura 4.25: Escaneo de Servicios con NMAP (Hosts: 20)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

```
Nmap scan report for 10.87.151.187
Host is up, received arp-response (0.00098s latency).
Not shown: 996 closed tcp ports (reset)
PORT    STATE SERVICE  REASON         VERSION
22/tcp  open  ssh      syn-ack ttl 64 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp  open  http     syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
111/tcp open  rpcbind  syn-ack ttl 64 2-4 (RPC #100000)
443/tcp open  ssl/http syn-ack ttl 64 Apache httpd 2.4.41 ((Ubuntu))
MAC Address: 00:50:56:94:F6:35 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.87.151.190
Host is up, received arp-response (0.0011s latency).
Not shown: 968 filtered tcp ports (no-response), 31 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.4 (protocol 2.0)
MAC Address: 00:50:56:94:3A:47 (VMware)

Nmap scan report for 10.87.151.191
Host is up, received arp-response (0.00092s latency).
Not shown: 968 filtered tcp ports (no-response), 31 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.4 (protocol 2.0)
MAC Address: 00:50:56:94:11:49 (VMware)

Nmap scan report for 10.87.151.192
Host is up, received arp-response (0.0010s latency).
Not shown: 967 filtered tcp ports (no-response), 32 filtered tcp ports (host-prohibited)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 7.4 (protocol 2.0)
MAC Address: 00:50:56:94:74:A2 (VMware)

Nmap scan report for 10.87.151.193
Host is up, received arp-response (0.00095s latency).
Not shown: 964 filtered tcp ports (no-response), 32 filtered tcp ports (host-prohibited)
PORT     STATE  SERVICE    REASON         VERSION
22/tcp   open   ssh        syn-ack ttl 64 OpenSSH 7.4 (protocol 2.0)
80/tcp   closed http       reset ttl 64
443/tcp  open   ssl/http   syn-ack ttl 64 nginx
8080/tcp open   http-proxy syn-ack ttl 64 HAProxy http proxy 1.3.1 or later
MAC Address: 00:50:56:94:4C:66 (VMware)
Service Info: Device: load balancer
```

Figura 4.26: Escaneo de Servicios con NMAP (Hosts: 187, 190 – 193)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

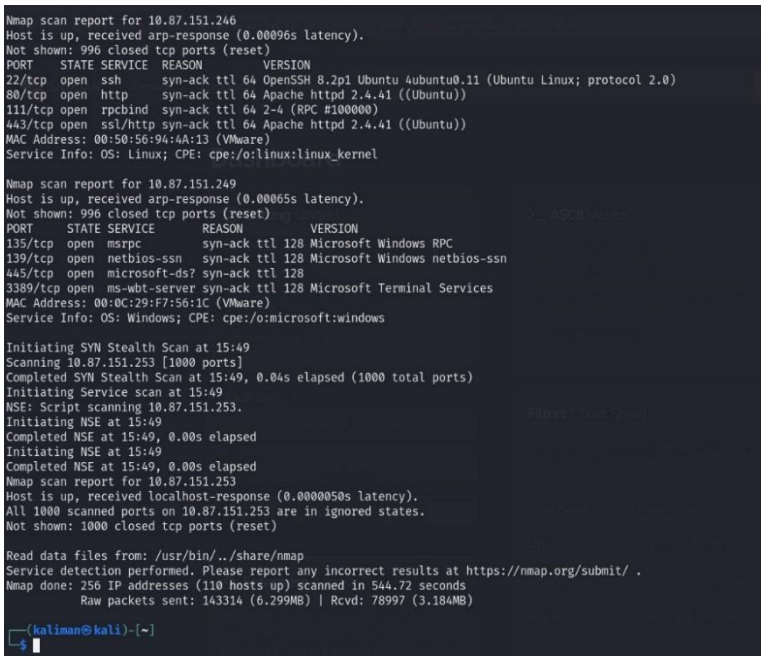


Figura 4.27: Escaneo de Servicios con NMAP (Hosts: 246, 249 y 253)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Nmap: SMB Enumeration

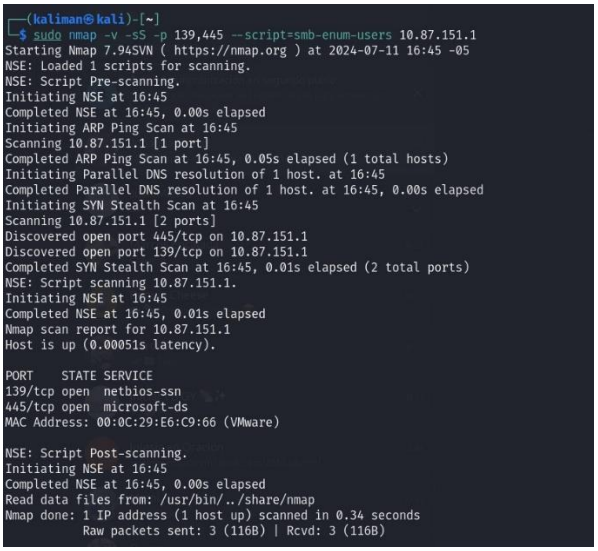


Figura 4.28: SMB Enumeration Users (Host: 1)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

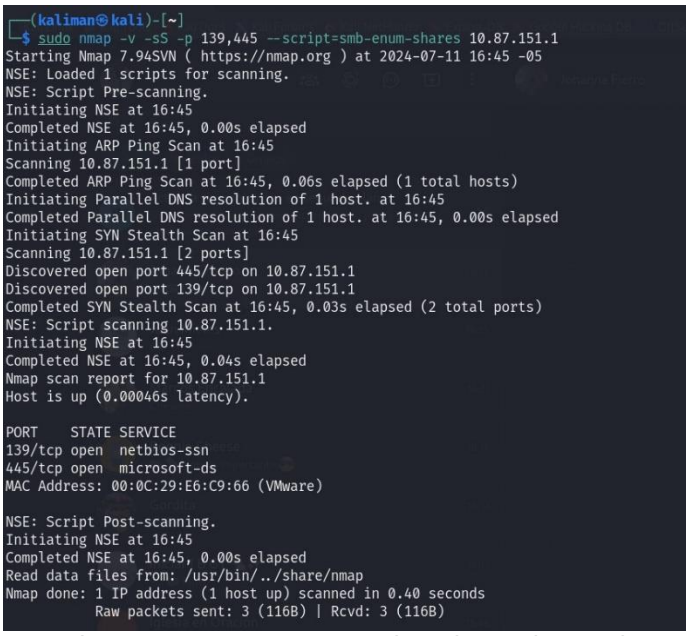


Figura 4.29: SMB Enumeration Shares (Host: 1)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

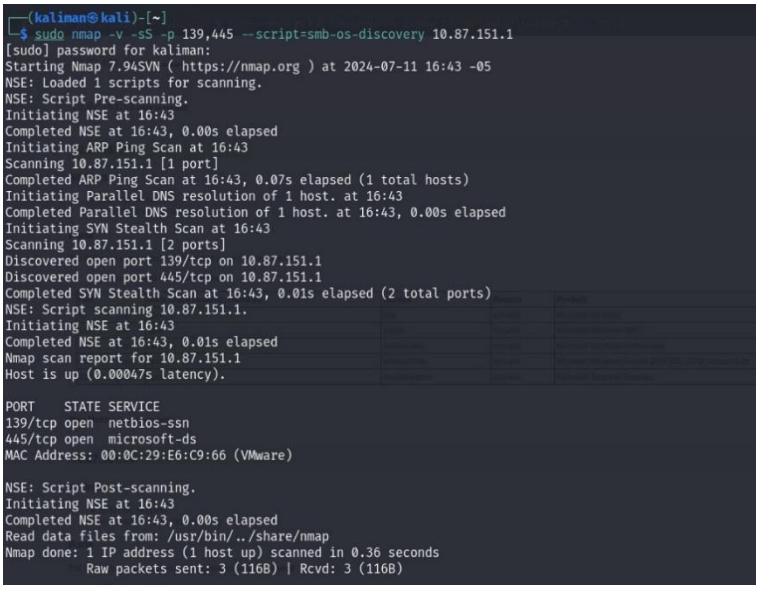


Figura 4.30: SMB Enumeration SO (Host: 1)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

Nmap: SNMP Enumeration

```
┌──(kaliman㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -v -sU -p 161 10.87.151.210
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 17:04 -05
Initiating ARP Ping Scan at 17:04
Scanning 10.87.151.210 [1 port]
Completed ARP Ping Scan at 17:04, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:04
Completed Parallel DNS resolution of 1 host. at 17:04, 0.00s elapsed
Initiating UDP Scan at 17:04
Scanning 10.87.151.210 [1 port]
Discovered open port 161/udp on 10.87.151.210
Completed UDP Scan at 17:04, 0.15s elapsed (1 total ports)
Nmap scan report for 10.87.151.210
Host is up (0.00091s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 00:00:5E:00:01:C9 (Icann, Iana Department)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
           Raw packets sent: 3 (195B) | Rcvd: 2 (155B)

┌──(kaliman㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Figura 4.31: SNMP Enumeration (Host: 210)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

```
┌──(kaliman㉿kali)-[/usr/share/nmap/scripts]
└─$ ls snmp*
snmp-brute.nse        snmp-info.nse        snmp-ios-config.nse  snmp-processes.nse  snmp-win32-services.nse  snmp-win32-software.nse
snmp-hh3c-logins.nse  snmp-interfaces.nse  snmp-netstat.nse     snmp-sysdescr.nse   snmp-win32-shares.nse    snmp-win32-users.nse

┌──(kaliman㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -v -sU -p 161 --script=snmp-win32-software 10.87.151.210
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-11 17:06 -05
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:06
Completed NSE at 17:06, 0.00s elapsed
Initiating ARP Ping Scan at 17:06
Scanning 10.87.151.210 [1 port]
Completed ARP Ping Scan at 17:06, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:06
Completed Parallel DNS resolution of 1 host. at 17:06, 0.00s elapsed
Initiating UDP Scan at 17:06
Scanning 10.87.151.210 [1 port]
Discovered open port 161/udp on 10.87.151.210
Completed UDP Scan at 17:06, 0.16s elapsed (1 total ports)
NSE: Script scanning 10.87.151.210.
Initiating NSE at 17:06
Completed NSE at 17:06, 5.00s elapsed
Nmap scan report for 10.87.151.210
Host is up (0.00089s latency).

PORT    STATE SERVICE
161/udp open  snmp
MAC Address: 00:00:5E:00:01:C9 (Icann, Iana Department)

NSE: Script Post-scanning.
Initiating NSE at 17:06
Completed NSE at 17:06, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.47 seconds
           Raw packets sent: 3 (195B) | Rcvd: 2 (155B)

┌──(kaliman㉿kali)-[/usr/share/nmap/scripts]
└─$
```

Figura 4.32: SNMP Enumeration Software
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

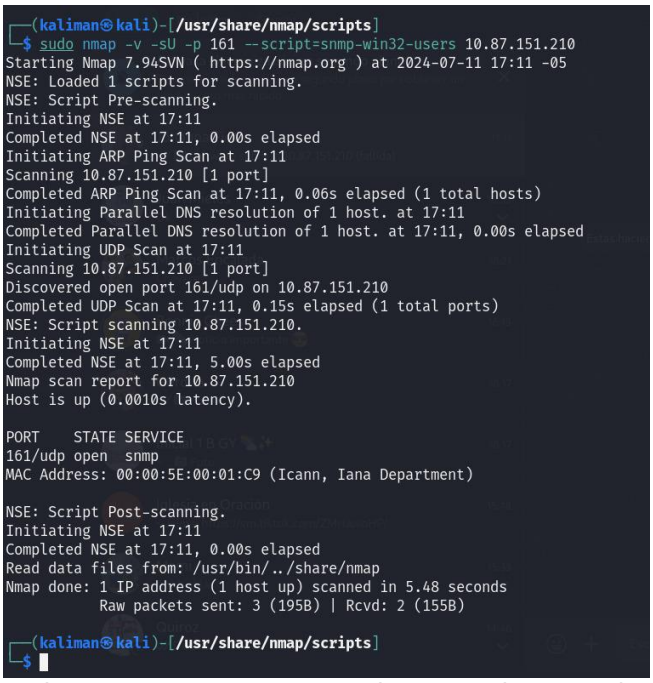


Figura 4.33: SNMP Enumeration Users (Host: 210)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

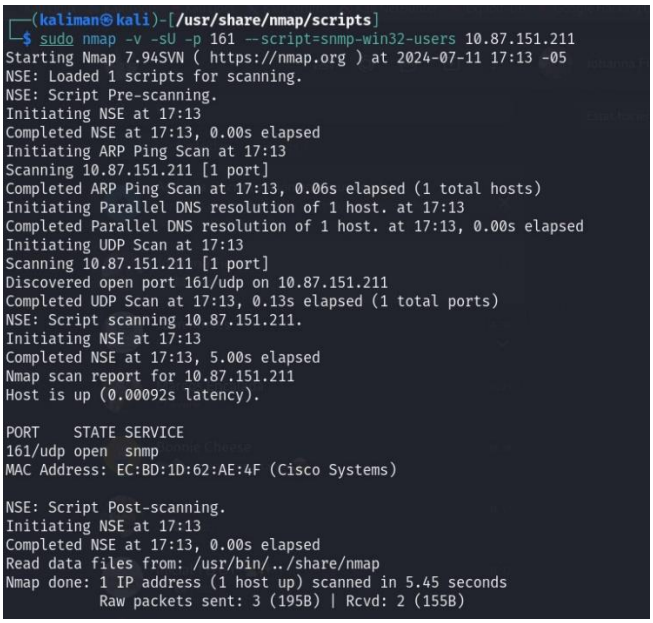


Figura 4.34: SNMP Enumeration Users (Host: 211)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

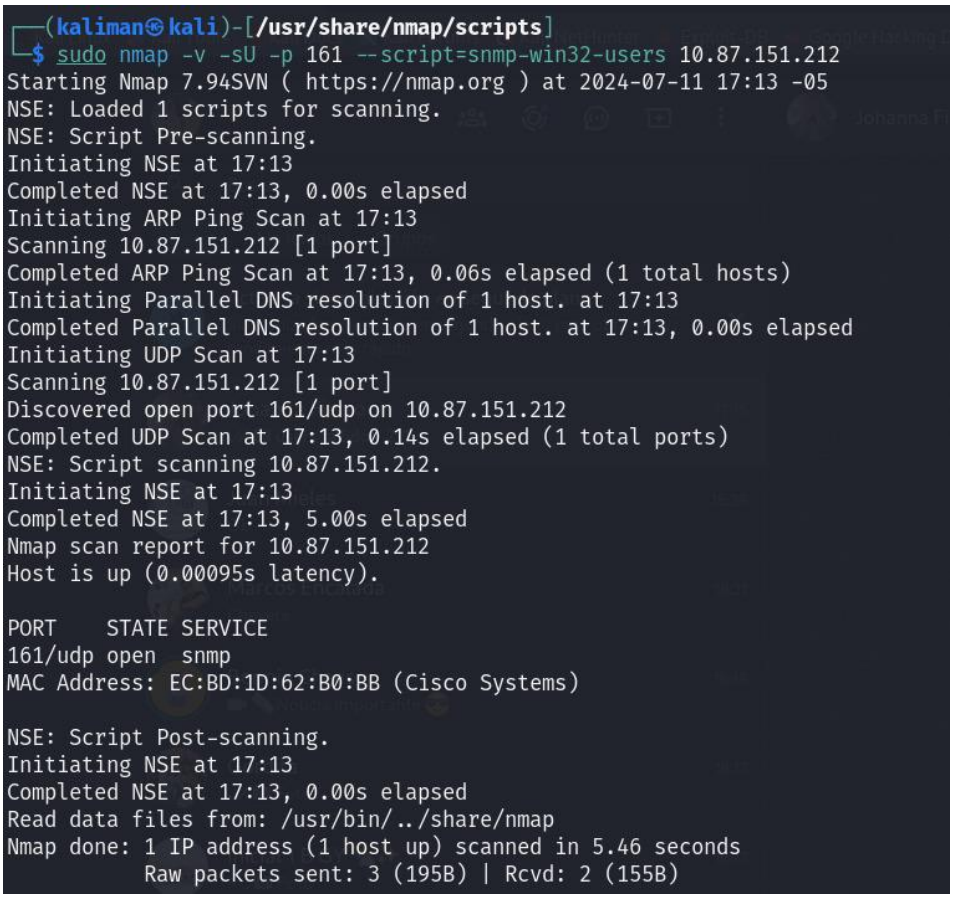


Figura 4.35: SNMP Enumeration Users (Host: 212)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

4.1.4. ANÁLISIS DE VULNERABILIDADES

Esta fase consiste en la identificación de fallos de seguridad que se encuentran presentes en los sistemas que se están evaluando. El tipo de fallos abarca desde errores en la configuración de un servicio hasta vulnerabilidades en determinados servicios que sean públicos y puedan comprometer la integridad del mismo.

Figura 4.36: Escaneo de Vulnerabilidades con Nessus
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

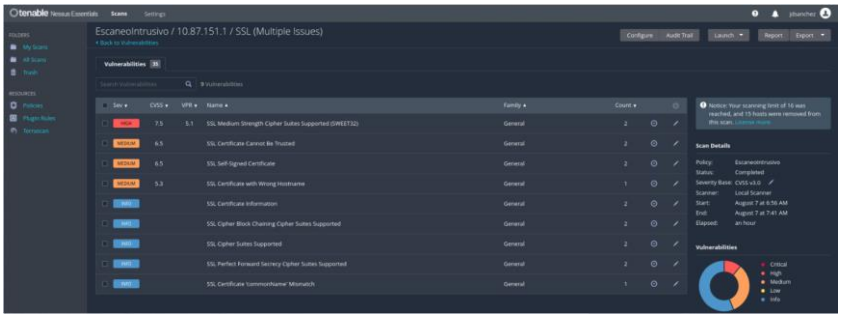


Figura 4.37: Escaneo de Vulnerabilidades con Nessus (Host: 1)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

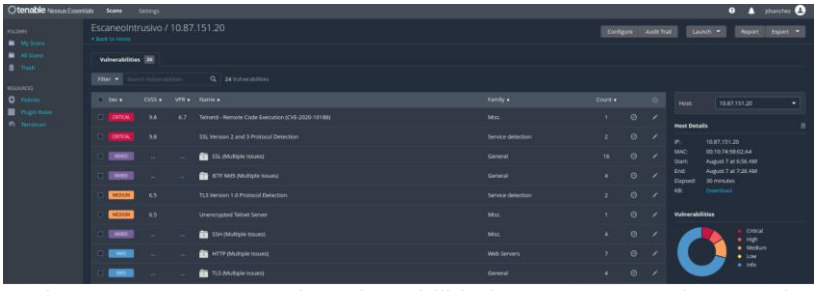


Figura 4.38: Escaneo de Vulnerabilidades con Nessus (Host: 20)
Fuente: Elaborado por Johanna Fierro y Josué Sánchez

CAPÍTULO V

DESARROLLO DEL PLAN DE MEJORA DE SEGURIDAD INFORMÁTICA EN LA RED WIFI DE LA INSTITUCIÓN EDUCATIVA.

5.1. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN (ISO 27001).

Definitivamente, implementar un plan de seguridad es fundamental para proteger la información y los activos de una organización. Es por ello, que es necesario desarrollar una política de seguridad de la información que garantice que la Institución proteja adecuadamente sus activos digitales; esta política de seguridad de la información debe redactarse de forma general, evitando el uso de términos técnicos, lo que permitirá que sea fácilmente entendida por todas las partes implicadas.

Finalmente, esta política deberá en lo posible cumplir con el requisito 5.2 de la NORMA ISO 27001.

5.2. POLÍTICAS ESPECÍFICAS RECOMENDADAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN.

Con la información recopilada durante la entrevista, encuesta y análisis de vulnerabilidades, se sugieren las siguientes políticas de Seguridad de la información para el mejor desarrollo del trabajo diario de la Institución Educativa.

5.2.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La Organización de la Seguridad de la información se refiere a la estructura y los procesos que una entidad establece para gestionar y proteger la información de manera efectiva.

El objetivo principal es conformar quienes serán parte del Directorio de Seguridad de la Información, que será el encargado de proporcionar dirección estratégica y supervisión en todas las cuestiones relacionadas con la seguridad de la información. Además, establecer cuáles son sus funciones, como, por ejemplo, crear las políticas específicas adecuadas a cada Departamento de la Institución Educativa, desarrollo de las estrategias a largo plazo que se llevaran a cabo para proteger la seguridad de la información, asignación de los recursos financieros y humanos para implementar medidas de seguridad de la información efectivas.

5.2.2. GESTIÓN DE ACTIVOS.

Inventario de activos

El inventario de activos pertenecientes a la Institución lo realiza el departamento de TI, quienes se encargan de registrar cualquier activo existente en todos los procesos existentes. Se realiza la transferencia de bienes para quienes entraron y salieron de la empresa.

El personal a quien se le entregan los activos informáticos es responsable y se le informa verbalmente que un activo específico queda a su debido cargo según los lineamientos de entrega de los activos. Por lo tanto, el departamento de TI no tiene custodia sobre todos los computadores informáticos que se encuentran en la institución.

Propiedad de los activos

Los bienes se adquieren a través del presupuesto de la institución según las necesidades de cada proceso interno o externo y son propiedad de la Universidad.

El departamento de TI gestiona el cuidado de los bienes informáticos de la organización y los designa como custodios al personal al entregarlos o al ingresarlos.

Devolución de activos

Este control tiene en cuenta el estado de los activos de los empleados o terceros que hayan finalizado su trabajo para la institución. Se siguen las cláusulas de devolución de activos físicos y/o electrónicos que se informaron al personal antes de la entrega.

5.2.3. MANIPULACIÓN DE LOS SOPORTES.

Gestión de soportes extraíbles

El personal está familiarizado con el uso de soportes extraíbles, porque son un componente crucial en la seguridad de la información. Sin embargo, no se proporcionan bloqueos sobre los puertos para que el medio extraíble no pueda usarse.

Eliminación de soportes.

No hay métodos seguros de borrado de datos de los soportes después de que hayan terminado su ciclo de vida. La información solo se borra de acuerdo con el estado del activo y el tiempo disponible para un integrante del área de TI. Como resultado, el activo que no agrega valor se da de baja y un miembro de la empresa o un tercero puede recuperar información confidencial utilizando los programas de recuperación de datos disponibles.

5.2.4. CONTROL DE ACCESO.

Requisitos de negocio para el control de acceso

Política de control de acceso

Aunque no hay políticas establecidas para la gestión del control de acceso, hay procedimientos que ayudan a llevar a cabo este control. Por ejemplo, un empleado no puede acceder a una computadora que no está bajo su cargo, ni mucho menos a los sistemas que maneja la Institución si no tiene los permisos adecuados. El departamento de TI otorga claves para controlar este proceso.

Acceso a las redes y a los servicios de red

El Departamento de TI restringe el acceso del personal a servicios que no son necesarios para el desarrollo y cumplimiento de las actividades laborales, así como a sitios web que no sean autorizados y que no sean seguros. También mantienen requisitos de autenticación para el acceso a las redes.

Gestión de acceso de usuario

Registro y baja de usuario.

El departamento de TI es responsable de administrar los registros y bajas de usuarios de la Institución.

Los jefes de cada área son los encargados de solicitar al departamento de sistemas la creación y asignación de una cuenta para el empleado que se encuentra en su proceso de ingreso, o eliminar usuarios en los sistemas.

Para la gestión de usuarios en computadoras, el personal de TI es responsable de crear o modificar a un usuario con sus credenciales correspondientes.

Gestión de la información secreta de autenticación de los usuarios

El departamento de TI informa verbalmente sobre la importancia de mantener la confidencialidad de las contraseñas para la autenticación de los usuarios de la Institución. Además, informa que el cambio de contraseña es crucial después de que se le proporcione una contraseña genérica, que es temporal.

Un problema identificado es que el usuario no ha recibido capacitación o instrucciones sobre cómo crear contraseñas, lo que pone en peligro la seguridad de las contraseñas.

Retirada o adaptación de los derechos de acceso.

Este control se da cuando hay cambios en los puestos de trabajo o cuando algún miembro de la empresa termina su cargo o trabajo. Se quitan todos los derechos de acceso a la información y a los recursos de tratamiento de información.

Responsabilidades del usuario

Uso de la información secreta de autenticación

El departamento de TI enseña al personal de la Institución la importancia del uso de la autenticación confidencial con varios parámetros (no revelar información, contraseñas seguras y fáciles de recordar...). Pero debido a que solo son mensajes informativos y no existe un control formal, el cumplimiento sigue siendo ineficiente.

5.2.5. SEGURIDAD FÍSICA Y DEL ENTRONO

Áreas seguras

Controles físicos de entrada

La empresa contratada de seguridad controla el acceso a la Institución para evitar intrusos, el personal que trabaja en la Institución se identifica con una credencial y se registra en el biométrico, mientras que las

personas que no son parte de la institución se verifican y retienen su cedula de identidad para su posible ingreso, y el registro de visitas.

Cuando alguien desea salir de la empresa, el guardia se encarga de hacer una revisión física y a la vez registra ingresos y salidas de todo personal entrante y saliente de la Institución.

Seguridad de oficinas, despachos y recursos

Los accesos de entrada y salida de las diferentes áreas existentes se controlan mediante oficiales de seguridad, así se evitan posibles riesgos de la información, pero no toman énfasis los activos de información almacenados por parte de los usuarios.

Protección contra las amenazas externas y ambientales

La Institución cuenta con señales de advertencia en áreas visibles para que el personal y los visitantes tengan conocimiento de dónde deben dirigirse en caso de emergencia.

En caso de incendios, se ha establecido un sistema de alarma contra incendios que, si se activa, todos los que se encuentren en la institución deben retirarse inmediatamente de la zona de peligro y encaminarse al punto de encuentro seguro.

Se dispone de extintores en áreas estratégicas de la Institución, ubicados en planta en cada piso, y disponibles para aquellos que los necesiten en ese momento. Actualmente, la matriz de la empresa consta de tres pisos, lo que dificulta la evacuación en caso de emergencia para personas con discapacidad.

Seguridad de los equipos

Emplazamiento y protección de equipos

La Institución cuenta con un espacio denominado Data Center en el que alberga sus equipos de comunicaciones. El lugar se encuentra ambientado para que los sistemas trabajen de forma adecuada.

Adicional, cuentan con un sistema de UPS para la protección de energía eléctrica.

Instalaciones de suministro

En los departamentos y otras áreas donde hay equipos electrónicos, hay sistemas UPS que tienen la capacidad de alimentar los equipos durante el tiempo necesario para que los empleados puedan proteger sus actividades en caso de una falla eléctrica.

Se demostró que, de acuerdo con las especificaciones de los fabricantes, no existe un plan de mantenimiento para UPS.

Un problema con respecto a los UPS es que como ya se mencionó que no se tiene un plan de mantenimiento, en consecuencia existen fallos de que el sistema de UPS se encuentre defectuoso o que prácticamente deje de funcionar.

Seguridad del cableado

En los puntos donde se requiere conexión, se utiliza cable UTP categoría 5e y 6 con conectores RJ45. Es importante mencionar que en la mayoría de los racks de la Institución el cableado no se encuentra correctamente

etiquetado y organizado, lo cual podría ocasionar problemas de lazos y pérdidas de enlaces.

Mantenimiento de los equipos.

Se tuvo conocimiento de que no hay un plan de mantenimiento programado para los servidores; el mantenimiento se realiza cuando los servidores presentan problemas, no funcionan correctamente o han estado sin mantenimiento durante un período prolongado de tiempo. El personal de TI es responsable de realizar el mantenimiento.

Para los equipos de comunicaciones (CPE, Firewalls, Switch, Wi-Fi) existen contratos estipulados donde el mantenimiento se tiene al menos una vez al año.

Política de puesto de trabajo despejado y pantalla limpia

El departamento de TI solo ha aplicado este control de manera informativa, pero no ha implementado políticas que ayuden al cumplimiento, lo que resulta en inconvenientes como el mal uso de activos de información, un puesto de trabajo desordenado y con facilidad de visualización de la información que se maneja en cada área de trabajo.

5.2.6. SEGURIDAD DE LAS OPERACIONES

Protección contra el software malicioso (malware)

Controles contra el código malicioso

Se basan en anuncios informativos y control mediante antivirus, que se utilizan para contrarrestar códigos maliciosos.

No hay reglas que impidan que los usuarios de computadoras utilicen la herramienta antimalware al ingresar sus medios de almacenamiento.

Existe un alto riesgo de robo de información porque no se toman medidas adecuadas para identificar ni contrarrestar códigos maliciosos.

Control del software en explotación

Instalación del software en explotación

El departamento de TI instala software en todos los dispositivos de la empresa mediante procedimientos y no políticas establecidas. Es importante destacar que el departamento de sistemas es el único que puede instalar el software, ya que no se maneja con la aprobación de la gerencia.

El software instalado se examina para garantizar que funcione correctamente en portátiles, servidores y bases de datos.

Además, se considera la instalación de software que soporta, debido a que se rigen por sus habilidades. Solo el personal de sistemas puede instalar el software.

5.2.7. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Responsabilidades y procedimientos

El departamento de TI es responsable de resolver problemas relacionados con la tecnología para gestionar incidentes y mejoras de la seguridad de la información, pero no se han establecido procedimientos

o responsables del departamento de sistemas para implementar medidas de seguridad.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. En esta Institución se tiene poco conocimiento de la seguridad de información y esta es la principal razón por la cual no poseen procesos con políticas de control eficaces que garanticen la integridad, confidencialidad y disponibilidad de la información.
2. El desarrollo del Plan de Seguridad lo basamos en la Norma ISO 27001, con esta guía procedimos a realizar la propuesta para la Institución educativa con los controles más adecuados para la seguridad de la información.
3. Actualmente se ha tomado conciencia de la importancia de la seguridad de la información en las labores diarias, y están haciendo mejoras.
4. Se puede identificar que muchos de los servicios que corren sobre los servidores se encuentran sobre puertos TCP conocidos.

5. Se pudo evidenciar que los sistemas operativos de los servidores se encuentran trabajando en sistemas operativos Windows y Ubuntu. Adicional, las versiones de estos sistemas operativos se encuentran en versiones donde existen brechas de seguridad.

6. Se evidenció que existen debilidades en la seguridad de códigos remotos al existir desbordamiento de búfer en telnetd debido a comprobaciones de límites incorrectas en el manejo de servicios de escrituras cortas y datos urgentes.

7. En el proceso de hacking ético, se pudo evidenciar que en la red no existe un equipo que pueda identificar el tráfico inusual que se genera al escanear la red.

8. Se identificó que, para la mayoría de los servidores de la red, se tienen los mismos servicios aperturados y versiones instaladas.

RECOMENDACIONES

1. Sugerir a la Gerencia del departamento de TI de la Institución para que se evalué la creación de un departamento de Seguridad.

2. Establecer políticas claras sobre el uso de dispositivos de almacenamiento en la organización.

3. Implementar software que permita gestionar y controlar qué dispositivos USB pueden conectarse al sistema.

4. Realizar mantenimientos preventivos tanto a nivel físico como lógico de los componentes que conforman la red.

5. Implementar sistemas de detección (IDS) y prevención de intrusiones (IPS) para proteger la infraestructura de red y los sistemas informáticos.

6. Realizar capacitaciones al personal, a fin de que se familiaricen con los procedimientos de seguridad de la organización, incluyendo cómo manejar información confidencial y cómo responder a incidentes de seguridad.

BIBLIOGRAFÍA

[1] F. Juca-Maldonado y R. Medina-Peña, «Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas.», Portal Cienc., vol. 4, n.o 3, pp. 325-337, 2023.

[2] «Ataques cibernéticos amenazan seguridad en Ecuador», Diálogo Américas.

Accedido: 21 de octubre de 2023. [En línea]. Disponible en: https://dialogoamericas.com/es/articles/ataques-ciberneticos-amenazan-seguridad-en-ecuador/

[3] «The Political Cybersecurity Blindfold in Latin America», Default. Accedido: 21 de octubre de 2023. [En línea]. Disponible en: https://www.lawfaremedia.org/article/thepolitical-cybersecurity-blindfold-in-latin-america

[4] C. A. D. Clavijo, «Políticas de seguridad informática», Entramado, vol. 2, n.o

1, pp. 86-92, 2006.

[5] C. F. Martínez Cáceres y O. M. Oñate Haro, «Mejoras en la seguridad de la red

inalámbrica de la Universidad Nacional de Chimborazo aplicando hacking ético.»,

B.S. thesis, Riobamba, Universidad Nacional de Chimborazo, 2017.

[6] I. E. BRIONES CASTRO, «APLICACIÓN DE HACKING ÉTICO PARA LA

DETERMINACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES EN LA RED DE LA UNIVERSIDAD ESTATAL DEL SUR DE MANABÍ», B.S. thesis, Jipijapa. UNESUM, 2020.

[7] F. Kitsios, E. Chatzidimitriou, y M. Kamariotou, «The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector», Sustainability, vol. 15, n.o 7, p. 5828, 2023.

[8] M. M. Jiménez, «Conoce la importancia de tener un plan de seguridad de la información». Accedido: 21 de octubre de 2023. [En línea]. Disponible en: https://www.piranirisk.com/es/blog/importancia-plan-seguridad-de-informacion