REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN MENCIÓN EN SEGURIDAD INFORMÁTICA

TITULO DEL TRABAJO DE TITULACIÓN

"TESTEO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVIDORES DE BORDE DE LOS ISPS EN LA EMPRESA AIRMAXTELECOM S.A. MEDIANTE LA GUÍA NIST SP 800-115"

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con Mención en Seguridad Informática

AUTOR:

JONATHAN JAVIER SILVA MORAN

DIRECTOR:

MSc. MAURICIO XAVIER REA PEÑAFIEL

Ibarra, diciembre 2024

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Acreditada Resolución Nro. 173-SE-33-CACES-2020

BIBLIOTECA UNIVERSITARIA

UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	0401769989		
APELLIDOS Y NOMBRES	SILVA MORAN JONATHAN JAVIER		
DIRECCIÓN	EL CARMELO – CARCHI – ECUADOR		
EMAIL	jxsilvam@utn.edu.ec		
TELÉFONO FIJO	3014719	**TELÉFONO MÓVIL:**	0963929315

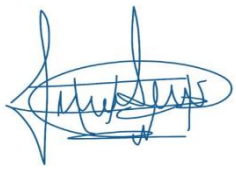
DATOS DE LA OBRA	
TÍTULO:	TESTEO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVIDORES DE BORDE DE LOS ISPS EN LA EMPRESA AIRMAXTELECOM S.A. MEDIANTE LA GUÍA NIST SP 800-115
AUTOR (ES):	SILVA MORAN JONATHAN JAVIER
FECHA:	10/12/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA	**GRADO** **POSGRADO X**
TITULO POR EL QUE OPTA	MAESTRÍA EN COMPUTACION MENCION EN SEGURIDAD INFORMÁTICA
TUTOR	**MSC. MAURICIO XAVIER REA PEÑAFIEL**

2. CONSTANCIAS

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

Ibarra, a los 10 días del mes de diciembre del 2024

EL AUTOR:



Firma_____

Nombre: Ing. Silva Moran Jonathan Javier

Ibarra, 23 de octubre de 2024

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado "TESTEO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVIDORES DE BORDE DE LOS ISPS EN LA EMPRESA AIRMAXTELECOM S.A. MEDIANTE LA GUÍA NIST SP 800-115", del maestrante **SILVA MORAN JONATHAN JAVIER**, de la Maestría de Computación Mención en Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	MSc. Rea Peñafiel Mauricio	XAVIER MAURICIO REA PEÑAFIEL
Asesor/a	MSc. Farinango Endara Henry	HENRY PATRICIO FARINANGO ENDARA

DEDICATORIA

A Dios, por ser mi guía, fuente de fortaleza y sabiduría durante este arduo proceso. A lo largo de los momentos difíciles y los desafíos, Su luz y gracia me han permitido seguir adelante con determinación y esperanza. Todo lo que soy y todo lo que he logrado es gracias a Su infinita bondad.

A mi familia, por su amor incondicional, su apoyo constante y su fe en mí. A mis padres, quienes me inculcaron los valores del esfuerzo y la perseverancia, y a mis hermanos, que siempre han estado a mi lado, brindándome ánimos y comprensión. Este logro es tanto suyo como mío, pues sin ustedes este camino habría sido mucho más difícil.

TABLA DE CONTENIDO

EL PROBLEMA **10**

1.1 Problema de investigación 10

1.2 Objetivos de la investigación 11

1.2.1. Objetivo General 11

1.2.2. Objetivos Específicos 11

1.3. Justificación 12

CAPÍTULO II **15**

MARCO REFERENCIAL **15**

2.1. Antecedentes 15

2.2. Marco teórico 16

2.2.1. Servidores de Borde de ISP 16

2.2.2. Sistema de Gestión de Seguridad de la Información (SGSI): 17

2.2.3. Seguridad de la Información 17

2.2.4. Seguridad Informática y Sistema Informático 17

2.2.5. Manual de Políticas de Seguridad de la Información 18

2.2.6. Gestión de Riesgos en Seguridad de la Información 18

2.2.7. Delitos Informáticos, Hackers y Crackers 19

2.2.8. Virus Informáticos, Metodologías de Gestión de Riesgos 20

2.2.9. Metodología NIST SP 800-115 22

2.3. Marco legal 28

CAPÍTULO III **30**

MARCO METODOLÓGICO **30**

3.1. Descripción del área de estudio / Descripción del grupo de estudio 30

3.2. Enfoque y tipo de investigación 31

3.3. Procedimiento de la investigación 33

3.3.1. Fase1: Técnicas de identificación y análisis de objetivos 33

3.3.2. Fase2: Vulnerabilidad de destino Técnicas de validación 47

3.3.3. Fase 3: Propuesta de Mejoras y Estrategias de Seguridad 66

CAPÍTULO IV **70**

RESULTADOS Y DISCUSIÓN **70**

CONCLUSIONES Y RECOMENDACIONES **81**

REFERENCIAS Y BIBLIOGRAFIA **83**

ANEXOS **86**

ÍNDICE DE TABLAS

Tabla 1 ESCANEO DE PUERTOS DE LOS SERVIDORES 34
Tabla 2 RESUMEN TÉCNICAS DE IDENTIFICACIÓN Y ANÁLISIS 47
Tabla 3 PRUEBAS DE PENETRACION DE VULNERABILIDADES A SERVIDORES 56
Tabla 4 MEJORAS Y ESTRATEGIAS DE SEGURIDAD 67
Tabla 5 ¿Con qué frecuencia cambia las contraseñas de acceso a los sistemas críticos? 71
Tabla 6 ¿Con qué frecuencia se realizan respaldos de la información crítica en los servidores de borde? 72
Tabla 7 ¿Qué nivel de conocimiento tiene sobre los tipos de ataques cibernéticos a los que están expuestos los servidores de borde? 73
Tabla 8 ¿Cuándo fue su última capacitación formal sobre ciberseguridad y protección de sistemas? 74
Tabla 9 ¿Comparte las credenciales de acceso (usuario y contraseña) con otros compañeros de trabajo? 75
Tabla 10 ¿Qué tan claras y fáciles de seguir considera las políticas de seguridad de la información de la empresa? 76
Tabla 11 ¿Cómo calificaría la eficacia del sistema de protección contra ataques de denegación de servicio (DDoS)? 77
Tabla 12 ¿Con qué frecuencia se aplican actualizaciones de seguridad en los sistemas críticos? 78
Tabla 13 ¿Ha sido testigo o ha tenido conocimiento de intentos de ataque o brechas de seguridad en los servidores de borde en los últimos 12 meses? 79
Tabla 14 ¿Cómo calificaría la gestión general de la seguridad de la información en la empresa? 80

ÍNDICE DE FIGURAS

Figura 1 Problema de investigación 11
Figura 2 Fases de una prueba de intrusión. 25
Figura 3 Actividades específicas de la Fase de Ejecución. 26
Figura 4 Ubicación de AIRMAXTELECOM S.A. 30
Figura 5 Bloqueos por categorías de seguridad 32
Figura 6 Páginas web maliciosas bloqueadas 32
Figura 7 Análisis Vulnerabilidades - Servidor Ibarra. 39
Figura 8 Análisis Vulnerabilidades - Servidor Bolívar. 40
Figura 9 Análisis Vulnerabilidades - Servidor Pimampiro. 42
Figura 10 Análisis Vulnerabilidades - Servidor Urcuqui 43
Figura 11 Análisis Vulnerabilidades - Servidor Cotacachi 44
Figura 12 Análisis Vulnerabilidades - Servidor Otavalo 45
Figura 13 John The Ripper – Verificación de hash 49
Figura 14 Jhon The Ripper - Sin exito en las contraseñas. 49
Figura 15 Topología de Red AIRMAXTELECOM S.A. 53
Figura 16 Actualización de Kali 55
Figura 17 Clonacion de repositorio 55
Figura 18 Instalación Cmake 55
Figura 19 Instalación de Libboost 56
Figura 20 Compilación de códigos. 56
Figura 21 Ejemplo de credencial vulnerada 56
Figura 22 Solicitud de autorización. 59
Figura 23 Aceptación de la solicitud 60
Figura 24 Email enviado a los usuarios. 63

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCION EN SEGURIDAD INFORMÁTICA

TESTEO Y EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE LOS SERVIDORES DE BORDE DE LOS ISPS EN LA EMPRESA AIRMAXTELECOM S.A. MEDIANTE LA GUÍA NIST SP 800-115

Autor: Jonathan Javier Silva Moran
Director: Msc. Mauricio Rea
Año: 2024

RESUMEN

La evaluación de seguridad realizada en seis servidores de borde MikroTik para AIRMAXTELECOM S.A., basada en la metodología NIST SP 800-115, arrojó que la infraestructura de la empresa es mayormente sólida y bien mantenida, con medidas efectivas como la filtración de puertos y la conexión cableada en lugar de interfaces inalámbricas. Sin embargo, se identificaron áreas críticas que requieren atención, tales como la necesidad de mejorar las políticas de cambio de contraseñas, implementar autenticación multifactor y fortalecer las políticas de respaldo y capacitación en ciberseguridad.

Los resultados del análisis de vulnerabilidades revelaron algunos problemas en la gestión de SSL/TLS, especialmente en el servidor de Ibarra, y la vulnerabilidad ante ataques de phishing fue notable, con tres de seis administradores proporcionando credenciales completas en las pruebas realizadas. Las contraseñas complejas demostraron ser un punto fuerte, pero aún hay margen para mejoras en la concienciación de los empleados y la implementación de controles de seguridad más estrictos.

Se hicieron recomendaciones clave que incluyen la implementación de políticas de cambio de contraseñas más estrictas, autenticación multifactor, aumento en la frecuencia de respaldos de información crítica, capacitación continua en seguridad informática y la realización de simulaciones de ciberataques como medida educativa y preventiva.

Palabras Claves: NIST SP 800-115, Seguridad de servidores MikroTik, Análisis de vulnerabilidades

PROGRAMA DE MAESTRÍA EN COMPUTACIÓN MENCION EN SEGURIDAD INFORMÁTICA

TESTING AND EVALUATION OF INFORMATION SECURITY OF ISPs' EDGE SERVERS AT AIRMAXTELECOM S.A. USING THE NIST SP 800-115 GUIDE

Autor: Jonathan Javier Silva Moran
Director: Msc. Mauricio Rea
Año: 2024

ABSTRACT

The security assessment conducted on six MikroTik edge servers for AIRMAXTELECOM S.A., based on the NIST SP 800-115 methodology, revealed that the company's infrastructure is mostly robust and well-maintained, with effective measures such as port filtering and wired connections instead of wireless interfaces. However, critical areas requiring attention were identified, such as the need to improve password change policies, implement multi-factor authentication, and strengthen backup policies and cybersecurity training.

The results of the vulnerability analysis revealed some issues in SSL/TLS management, especially on the Ibarra server, and vulnerability to phishing attacks was notable, with three out of six administrators providing complete credentials in the tests conducted. Complex passwords proved to be a strong point, but there is still room for improvement in employee awareness and the implementation of stricter security controls.

Key recommendations were made, including the implementation of stricter password change policies, multi-factor authentication, increased frequency of critical information backups, continuous training in computer security, and conducting cyber-attack simulations as an educational and preventive measure.

Keywords: NIST SP 800-115, MikroTik server security, Vulnerability analysis

CAPÍTULO I

EL PROBLEMA

1.1 Problema de investigación

La seguridad de los servidores de borde de los ISP en AIRMAXTELECOM S.A. es insuficiente o vulnerable a ataques cibernéticos, lo que podría comprometer la integridad de la infraestructura de red y la confidencialidad de los datos de los clientes.

El problema se sitúa en el contexto de la seguridad de los servidores de borde de los ISP, específicamente en el caso de AIRMAXTELECOM S.A; si bien es cierto estos factores se deben considerar y ser abordados correctamente de tal forma que se puedan promover de forma adecuada los beneficios de contar con un servicio estable y proyectar un mecanismo que mitigue los riesgos asociados a los servicios de dotación y aprovisionamiento del servicio de internet en distintas zonas geográficas (MARK, 2014).

El problema radica en la insuficiencia de la seguridad de los servidores de borde de AIRMAXTELECOM S.A. Esta falta de seguridad los hace vulnerables a diversos ataques cibernéticos, incluyendo Denegación de Servicio (DDoS), acceso no autorizado, vulnerabilidades de software, fugas de datos, suplantación de identidad (phishing), malware y ransomware, ingeniería social, acceso físico no autorizado, falta de parcheo y actualizaciones, y deficiencias en la política de seguridad. En Ecuador se detecta que un cierto número de estas empresas no poseen los mecanismos necesarios para controlar y monitorear las posibles incidencias, así como las diferentes anomalías que se desarrollen en el escenario de vbfuncionamiento, escalamiento y control de amenazas (ALULEMA, 2018).

• Los incidentes de ciberseguridad en infraestructura de ISP han crecido de manera significativa y es necesario identificar las vulnerabilidades que necesitan una protección inmediata (Mauricio Palate & Avila-Pesantez, 2021). ¿Cómo evaluar y mejorar la seguridad de los servidores de borde de AIRMAXTELECOM S.A. para mitigar la vulnerabilidad a

ataques cibernéticos y proteger la integridad de la infraestructura de red y la confidencialidad de los datos de los clientes?

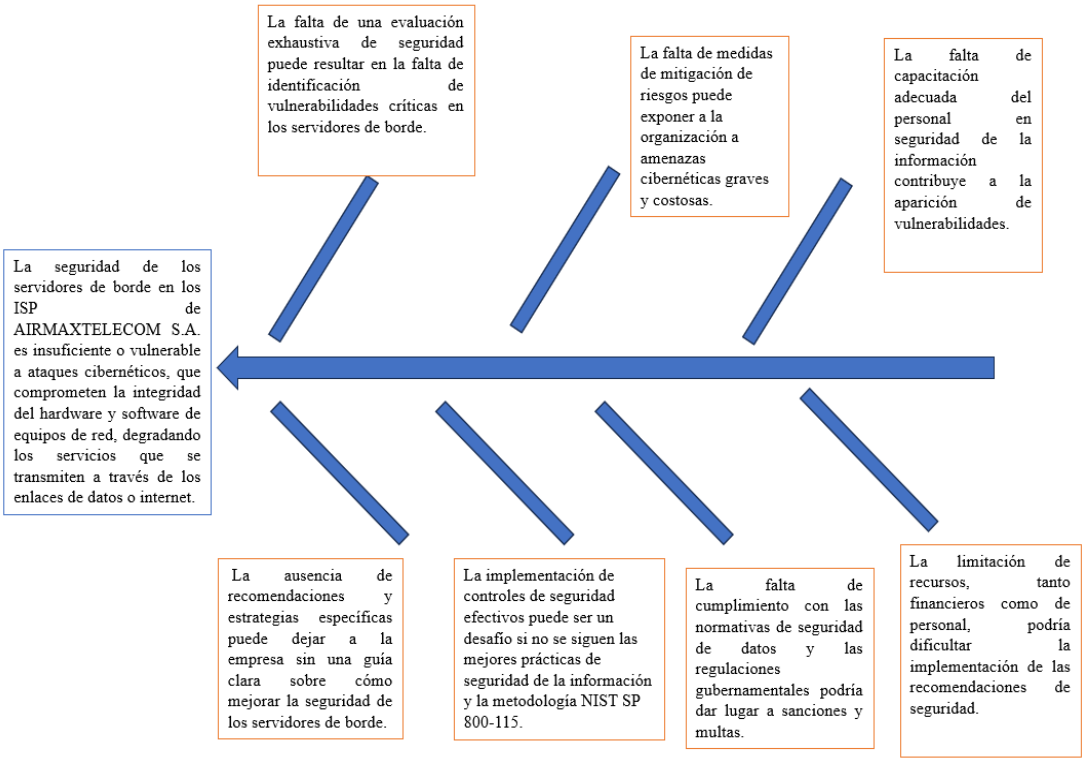


Figura 1 Problema de investigación
Fuente: Autor

1.2 Objetivos de la investigación

1.2.1. Objetivo General

- Evaluar la seguridad de los servidores de borde de los ISP en AIRMAXTELECOM S.A. mediante la aplicación de pruebas de penetración ética y el análisis de vulnerabilidades basado en la Guía NISP SP 800-115, con el fin de identificar posibles debilidades y proponer mejoras que fortalezcan la infraestructura de red.

1.2.2. Objetivos Específicos

- Identificar la infraestructura de los servidores de borde de los ISPS en AIRMAXTELECOM S.A.

- Encontrar las diferentes vulnerabilidades y verificar los ataques que se puedan realizar de acuerdo con la guía NIST SP 800-115.
- Proponer recomendaciones y estrategias específicas para mejorar la seguridad de los servidores de borde, incluyendo medidas de mitigación de riesgos y la implementación de controles de seguridad efectivos, basados en las mejores prácticas de seguridad de la información y la metodología NIST SP 800-115.

1.3. Justificación

Los proveedores de servicio de internet (ISP, por sus siglas en inglés) presentan un alto índice de vulnerabilidades respecto a la infraestructura de la red, en especial en los equipamientos de la red central (CORE), debido a que estos deben contrarrestar y mitigar cualquier tipo de ataque proveniente desde el internet o desde su propia red interna, para poder garantizar la confidencialidad, integridad y disponibilidad de los servicios (Shaikh, 2020).

En la era digital actual, los servidores de borde desempeñan un papel crucial en la conectividad de internet y en la distribución de servicios en línea. Dado el aumento constante de amenazas cibernéticas, incluyendo ataques sofisticados como el ransomware y el phishing, la seguridad de estos servidores se ha vuelto de suma importancia. La vulnerabilidad de los servidores de borde puede dar lugar a una serie de problemas, como la interrupción de los servicios, la pérdida de datos críticos y la exposición de información confidencial de los clientes, por otro lado, según la información levantada por el Centro de respuestas a incidentes informáticos Ecucert, el 43% de las empresas ISP que brindan los servicios de telecomunicaciones utilizan equipos Mikrotik (Ecucert, 2017).

AIRMAXTELECOM S.A. es una empresa que brinda servicios de Internet y telecomunicaciones a sus clientes. La seguridad de los servidores de borde es esencial para garantizar que los servicios que ofrecen sean confiables y seguros. Al abordar las

vulnerabilidades y mejorar la seguridad de estos servidores, se contribuye directamente a la protección de la infraestructura de red de la empresa, evitando interrupciones en los servicios y garantizando la confidencialidad de los datos de los clientes.

La implementación de mejores prácticas de seguridad de la información es esencial en el entorno digital actual. La metodología NIST SP 800-115 proporciona pautas valiosas para la evaluación de la seguridad de los sistemas de información. Al llevar a cabo esta investigación y aplicar esta metodología, se contribuye directamente a la mejora de las prácticas de seguridad de la información en AIRMAXTELECOM S.A. Además, puede ayudar a la empresa a cumplir con estándares y regulaciones de seguridad, lo que es fundamental para mantener la confianza de los clientes y cumplir con las leyes de protección de datos.

El objetivo del proyecto de investigación se alinea estrechamente con el Objetivo 1 del Eje 1 del Plan Nacional de Desarrollo de Ecuador, que busca 'garantizar una vida digna con iguales oportunidades para todas las personas' ([SEMPLADES], 2027). A través de la evaluación y mejora de la seguridad de los servidores de borde de AIRMAXTELECOM S.A., se está contribuyendo a crear un entorno en línea más seguro y equitativo para todos los ciudadanos y usuarios de servicios de Internet. Al fortalecer la ciberseguridad de estos servidores, se está trabajando para garantizar que todas las personas tengan igualdad de acceso a servicios en línea seguros y confiables, independientemente de su origen o ubicación. Este enfoque respalda directamente el objetivo de proporcionar igualdad de oportunidades y una vida digna para todos los ecuatorianos, como se establece en el Plan Nacional de Desarrollo (Secretaría Nacional de Planificación y Desarrollo) ([SEMPLADES], 2027).

Este proyecto de investigación tiene una significativa relevancia para la línea de investigación en Seguridad de la Información, línea de investigación de la maestría de computación con mención en ciberseguridad UTN. Al evaluar y mejorar la seguridad de los servidores de borde

de AIRMAXTELECOM S.A., se está abordando directamente las preocupaciones críticas en el campo de la seguridad de la información.

CAPÍTULO II

MARCO REFERENCIAL

2.1. Antecedentes

Un sistema es considerado seguro cuando satisface las cualidades de disponibilidad, integridad y confidencialidad de la información (Lopez, 2010). La seguridad de los sistemas de información es un aspecto crítico en la era digital actual, donde la información es un activo valioso y esencial para las organizaciones y las personas. Garantizar la disponibilidad, integridad y confidencialidad de los datos es fundamental para prevenir incidentes cibernéticos, proteger la privacidad de los usuarios y mantener la continuidad de las operaciones. La creciente interconexión de dispositivos y la dependencia de sistemas informáticos en diversas áreas, desde el sector empresarial hasta la atención médica y la educación, resaltan la necesidad apremiante de investigar y mejorar la seguridad de los sistemas de información. Además, en un mundo cada vez más globalizado, la seguridad cibernética se ha convertido en un tema de preocupación a nivel mundial, con repercusiones en la economía y la seguridad nacional. Por lo tanto, este proyecto de investigación busca abordar estas cuestiones críticas y contribuir al fortalecimiento de la seguridad de los sistemas de información en un entorno en constante evolución.

En investigaciones previas, se ha destacado la importancia crítica de garantizar la integridad, confidencialidad y disponibilidad de la información en el contexto de las telecomunicaciones. Por ejemplo, estudios como el de (Andersson, 2017), han identificado vulnerabilidades específicas en los servidores de borde de ISP que los hacen susceptibles a ataques cibernéticos, incluyendo Denegación de Servicio (DDoS) y accesos no autorizados. Estos hallazgos resaltan la necesidad de abordar las preocupaciones de seguridad en esta área.

Además, informes anuales de seguridad cibernética, como el proporcionado por la ENISA (European Union Agency for Cybersecurity) (Cybersecurity), s.f.) han señalado un aumento

en los incidentes de seguridad dirigidos a servidores de borde en la industria de las telecomunicaciones. Estos informes subrayan la creciente amenaza que enfrentan las empresas de telecomunicaciones en relación con la seguridad de sus servidores de borde.

La mitad de los enrutadores centrales utilizados en uno de los mayores intercambios de Internet del mundo son dispositivos MikroTik (Cerón, Scholten, Pras, & Santana, 2020). Esta estadística subraya la importancia y la penetración de los dispositivos MikroTik en la infraestructura crítica de las redes de Internet. La elección de estos dispositivos como componentes esenciales en un intercambio de Internet de tal envergadura es un testimonio de su eficiencia y versatilidad. Sin embargo, esta estadística también plantea interrogantes críticos en lo que respecta a la seguridad de estas redes vitales.

Sin embargo, a pesar de estos estudios, existe una falta de investigaciones específicas que evalúen y mejoren la seguridad de los servidores de borde en empresas de telecomunicaciones en Ecuador. Esto justifica la necesidad de este estudio, que se centrará en la evaluación de seguridad de los servidores de borde de AIRMAXTELECOM S.A. y en la propuesta de mejoras específicas basadas en las mejores prácticas de seguridad de la información y la metodología NIST SP 800-115.

2.2. Marco teórico

2.2.1. Servidores de Borde de ISP

Los servidores de borde de un Proveedor de Servicios de Internet (ISP) cumplen un rol crítico en la infraestructura de red. Estos servidores actúan como puntos de interconexión entre la red del ISP y la red de Internet. La seguridad de estos servidores es esencial para garantizar la operación ininterrumpida de la red y la protección de la información de los usuarios. Hoy en día el mundo de la gestión de red es muy importante ya que se ha generado la necesidad de saber que está pasando con los equipos que componen una red (Parias, 2016).

2.2.2. Sistema de Gestión de Seguridad de la Información (SGSI):

Un Sistema de Gestión de Seguridad de la Información permite la calidad de la seguridad de la información, gestionando el acceso a la información, brindando confidencialidad, disponibilidad e integridad a la información evitando ataques, filtración, alteración y pérdida de ingresos, cumpliendo con las normas legales (Villafuerte, 2014).

la implementación de un sistema de gestión de seguridad de la información busca establecer un marco de confianza en el ejercicio de sus deberes con el estado, los ciudadanos y clientes, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad (Agudelo, 2022).

2.2.3. Seguridad de la Información

La seguridad de la información ha evolucionado desde la seguridad física orientada a la protección de ordenadores a concentrarse en políticas, procedimientos y controles basados en las personas (Leidy Johanna Cárdenas Solano, 2016).

Las organizaciones están expuestas día a día a amenazas tanto internas como externas que ocasionan robo de identidad e información, bases de datos, información sensible de clientes, pérdida de credibilidad y daños financieros que pueden afectar la sostenibilidad de la entidad, por lo anterior, se cuestiona si las empresas conocen y aplican metodologías para el análisis de riesgos y protección de los principios de seguridad de la información o por el contrario desconocen los modelos que traigan protección de los principios de seguridad de la información (Ana Abril, 2013).

2.2.4. Seguridad Informática y Sistema Informático

La seguridad informática es importante e indispensable dentro de las empresas que trabajan digitalmente es por eso por lo que hay que darle la importancia necesaria y de manera

preventiva sería una de las mejores soluciones. La seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital (Buendía, 2013).

La seguridad informática es la disciplina que se ocupa de diseñar las normas procedimientos métodos y técnicas destinados a conseguir un sistema de información seguro y confiable (Aguilera, 2010).

2.2.5. Manual de Políticas de Seguridad de la Información

Es un conjunto de lineamientos, reglas, leyes y normas establecidas por la gerencia con ámbito legal, las cuales deben ser acatadas por todo el personal que utilice las tecnologías de la información y comunicación, con la finalidad de gestionar, controlar y salvaguardar la información (Orellana, 2021).

– IS0-27000: Esta es una norma Internacional dirigida para los Sistemas de Gestión de la Seguridad de la Información que permite evaluar riesgos para así mediante óptimos controles poder disminuir o eliminar riesgos y fortalecer la confidencialidad e integridad de los datos (Internet, 2019).

2.2.6. Gestión de Riesgos en Seguridad de la Información

Debido al rápido crecimiento de la tecnología, la información se ha vuelto más fácil de acceder, procesar, y usar ocasionando que presenten de manera más frecuente problemas en la seguridad de la información, que ponen en riesgo al activo más importante (la información) de toda la organización (Jiménez, 2021). A partir de esto, las instituciones establecen reglas y modelos de seguridad con el propósito de garantizar la disponibilidad, integridad y confidencialidad de los datos. Estas pautas de seguridad se fundamentan en enfoques y métodos diseñados para asegurar el adecuado desempeño de la información y la transferencia de datos entre usuarios.

Un marco de seguridad de la información es una serie de procesos documentados que a menudo se personalizan para resolver problemas específicos de seguridad de la información

(Leidy Johanna Cárdenas Solano, 2016). Estos marcos ofrecen directrices y prácticas recomendadas que pueden ser adaptadas según las necesidades y desafíos específicos de una organización. Al proporcionar un conjunto de procesos documentados, los marcos de seguridad de la información no solo ayudan a garantizar la confidencialidad, integridad y disponibilidad de los datos, sino que también permiten a las organizaciones mantenerse al día con las amenazas cibernéticas en constante evolución y responder de manera efectiva a incidentes de seguridad. En última instancia, estos marcos son una parte fundamental en la defensa contra las crecientes amenazas a la seguridad de la información en el mundo digital actual.

2.2.7. Delitos Informáticos, Hackers y Crackers

En la era digital, los delitos informáticos se han convertido en una preocupación creciente. Estos actos ilícitos, realizados a través del uso indebido de la tecnología, representan una amenaza constante para la privacidad y seguridad de la información de terceros. Los delincuentes cibernéticos, a menudo, se valen de tácticas sofisticadas para dañar, robar o acceder de manera no autorizada a datos almacenados en servidores y dispositivos electrónicos. Es fundamental comprender la magnitud de esta problemática y tomar medidas proactivas para salvaguardar la información en un mundo cada vez más interconectado. Los delitos informáticos, son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets (Acosta, 2020).

Hacker, como término, es comúnmente utilizado por los medios de comunicación para referirse a un intruso que irrumpe en los sistemas informáticos para robar o destruir datos (Richet, 2013). in embargo, es importante destacar que el término "hacker" abarca un espectro más amplio de habilidades y motivaciones en el mundo de la ciberseguridad. Los hackers pueden ser éticos, enfocados en identificar y solucionar vulnerabilidades en sistemas, o pueden ser maliciosos, buscando explotar esas mismas debilidades para fines personales o destructivos.

Esta diversidad de perfiles subraya la necesidad de comprender que no todos los hackers son delincuentes cibernéticos, y que la distinción entre "sombrero blanco" (hackers éticos) y "sombrero negro" (hackers maliciosos) es crucial en el ámbito de la seguridad informática.

Los crackers utilizan sus habilidades relacionadas con la seguridad informática para crear virus, troyanos, etc., e infiltrarse ilegalmente en sistemas seguros con la intención de dañar el sistema o con intenciones criminales y diferenciarlos del pirata informático original y no criminal (Richet, 2013). Es importante notar que, a menudo, se diferencia a los crackers del concepto original de piratas informáticos, quienes podían no tener intenciones criminales y se enfocaban en explorar y entender sistemas informáticos de manera constructiva. Esta distinción subraya la importancia de comprender las diferentes motivaciones y acciones dentro del vasto espectro de la ciberseguridad. Comúnmente los crackers entran en sistemas vulnerables y hacen daño ya sea robando información, dejando algún virus, malware, trojan en el sistema y crean puertas traseras para poder entrar nuevamente cuando les plazca (Quispe, 2010).

2.2.8. Virus Informáticos, Metodologías de Gestión de Riesgos

En la Real Academia nos encontramos con la siguiente definición del término virus: Programa introducido subrepticiamente en la memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada". "Se denomina virus informático a todo programa capaz de infectar a otros programas, a partir de su modificación para introducirse en ellos" (Hernández, 2003). Estos virus informáticos son una manifestación de la constante evolución de amenazas en el mundo digital. Su objetivo puede variar desde la alteración inofensiva de un sistema hasta la destrucción de datos cruciales. La capacidad de los virus para propagarse y mutar rápidamente hace que la seguridad de la información sea un tema crítico en la actualidad. La lucha contra estas amenazas requiere no solo de medidas reactivas, como el uso de software antivirus, sino también de enfoques proactivos, como la educación en

seguridad cibernética y la implementación de prácticas de seguridad sólidas en las organizaciones.

La seguridad de la información se ha vuelto esencial para empresas, organizaciones gubernamentales y particulares por igual. La gestión de riesgos de seguridad de la información desempeña un papel crucial en la protección de datos confidenciales, la prevención de amenazas cibernéticas y la garantía de la continuidad de las operaciones. Las metodologías de gestión de riesgos de seguridad de la información son enfoques estructurados y sistemáticos que permiten a las organizaciones identificar, evaluar y mitigar los riesgos que acechan a sus activos digitales. Estas metodologías proporcionan un marco sólido para abordar las complejidades de la ciberseguridad, ayudando a las organizaciones a tomar decisiones informadas y a salvaguardar sus datos en un mundo cada vez más interconectado y expuesto a amenazas constantes. En este contexto, exploraremos algunas de las metodologías más destacadas utilizadas para proteger la información en la era digital.

- ISO 27001: La norma ISO 27001 es un estándar internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Este sistema se utiliza para proteger la confidencialidad, integridad y disponibilidad de la información. La norma proporciona un marco para la seguridad de la información que ayuda a las organizaciones a identificar y gestionar sus riesgos de seguridad de la información de manera efectiva (GlobalSuit, 2023).
- NIST SP 800-30: La Guía Técnica para Evaluaciones y Pruebas de Seguridad de la Información NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment), fue publicada en septiembre del 2008 por el Instituto Nacional de Estándares y Tecnología (NIST) del gobierno de los EE.UU. Describe las pautas sobre cómo debe realizarse una Evaluación de Seguridad de la Información (ESI) y lo

conceptualiza como el proceso de determinar cuan eficazmente una entidad es evaluada frente a objetivos específicos de seguridad (Digital, 2017).

- MAGERIT: Es la metodología de análisis y gestión de riesgos elaborada en su día por el antiguo Consejo Superior de Administración Electrónica y actualmente mantenida por la Secretaría General de Administración Digital (Ministerio de Asuntos Económicos y Transformación Digital) con la colaboración del Centro Criptológico Nacional (CCN) (Administracion-Electronica, 2014).
- FAIR (Factor Analysis of Information Risk): Es un marco de riesgo reconocido globalmente al que organizaciones de todo tipo pueden consultar al identificar riesgos de información cibernética (wallarm, 2023).

2.2.9. Metodología NIST SP 800-115

La metodología NIST SP 800-115 Describe las pautas sobre cómo debe realizarse una Evaluación de Seguridad de la Información (ESI) y lo conceptualiza como el proceso de determinar cuan eficazmente una entidad es evaluada frente a objetivos específicos de seguridad. Define como activos y objetos de evaluación los servidores, redes de datos, procedimientos y personas (Digital, 2017).

En el contexto de la Evaluación de la Seguridad de la Información, existen tres enfoques de evaluación que pueden ser empleados:

- Pruebas: Consiste en someter uno o más elementos bajo evaluación a condiciones controladas. Con el objetivo de contrastar su comportamiento observado con las expectativas previas, permitiendo un análisis comparativo de los resultados.
- Escrutinio: Se trata de un proceso que implica examinar, inspeccionar, revisar, observar y analizar a fondo los objetos de estudio. Con el fin de profundizar en la comprensión

de los elementos evaluados, esclarecer dudas y recopilar información relevante que sirva como evidencia.

- Entrevista: Es el método que se basa en mantener comunicación directa con grupos de personas involucradas o relacionadas con el objeto de evaluación. Para obtener aclaraciones y recopilar testimonios que aporten evidencia significativa al proceso evaluativo.

La NIST SP 800-115 propone un proceso de Evaluación de Seguridad de la Información (ESI) que se compone, como mínimo, de tres etapas:

- Planificación: Esta etapa, considerada crítica para el éxito de la Evaluación de Seguridad de la Información, implica la recopilación de datos acerca de los activos a ser evaluados, las amenazas que afectan a dichos activos y los controles de seguridad que pueden ser utilizados para mitigar estas amenazas. Dado que una Evaluación de Seguridad de la Información se trata esencialmente de un proyecto, se requiere la formulación de un plan de gestión que abarque metas y objetivos específicos, el alcance del proyecto, los requisitos, la definición de roles y responsabilidades de los equipos involucrados, limitaciones, factores clave para el éxito, restricciones, asignación de recursos, planificación de tareas y entregables.
- Ejecución: La fase de ejecución tiene como objetivo principal la identificación de vulnerabilidades y su posterior verificación, siguiendo el plan de trabajo previamente establecido. En esta etapa se aplican métodos y técnicas de evaluación adecuados de acuerdo con los objetivos específicos de la Evaluación de Seguridad de la Información.
- Post-Ejecución: En esta etapa, el enfoque se centra en el análisis de las vulnerabilidades descubiertas con el fin de determinar sus causas subyacentes, formular recomendaciones para su mitigación y elaborar un informe final que resuma los hallazgos y las acciones recomendadas.

Este proceso de Evaluación de Seguridad de la Información ofrece una estructura sólida para garantizar que los controles de seguridad se ajusten de manera efectiva a los riesgos y amenazas en constante evolución en el entorno de la información.

Las pruebas de intrusión, según la NIST SP 800-115, se definen como evaluaciones de seguridad en las cuales los evaluadores simulan ataques del mundo real para identificar posibles maneras de evadir las características de seguridad de una aplicación, sistema o red de datos. Estas pruebas a menudo involucran la búsqueda de combinaciones de vulnerabilidades en uno o más sistemas, con el fin de explotarlas y obtener un nivel de acceso superior al que se lograría mediante la explotación de una única vulnerabilidad.

De acuerdo con el estándar NIST SP 800-115, las pruebas de intrusión ofrecen varias ventajas importantes:

- Permiten observar cómo reacciona el sistema ante situaciones de ataque reales.
- Ayuda a entender que nivel de habilidad necesitaría un atacante para vulnerar el sistema con efectividad.
- Identificar nuevas medidas de seguridad para proteger mejor el sistema contra amenazas.
- Evaluar la eficacia del equipo de defensa en la detección y respuesta a los ataques.

Fases de una prueba de intrusión:

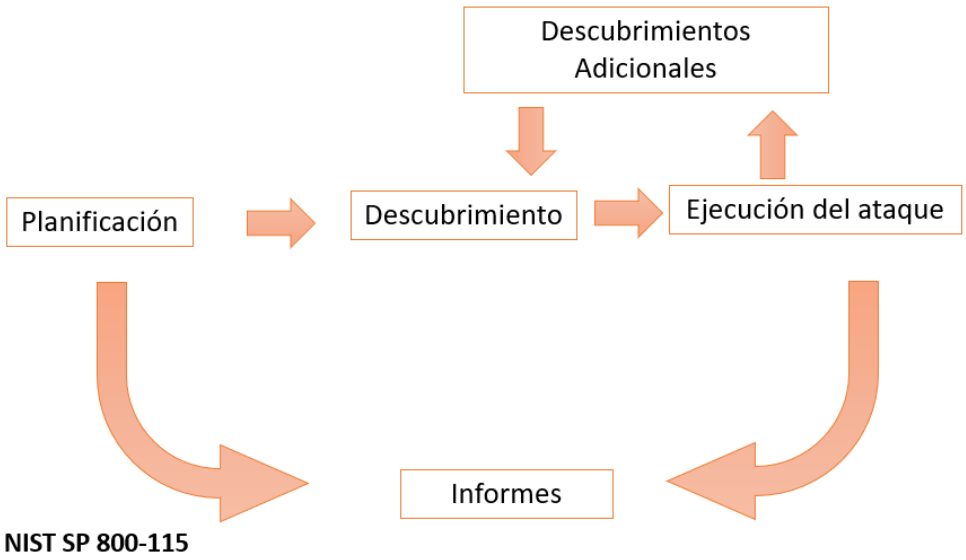


Figura 2 Fases de una prueba de intrusión.
Fuente: Estructura NIST SP 800-115

- Fase de Planificación: En esta etapa, se establecen las directrices que regirán todo el proceso, se definen con precisión los objetivos a alcanzar y se gestionan las aprobaciones necesarias para proceder. Simultáneamente, se preparan las condiciones técnicas y organizativas que garantizaran el éxito de la prueba. Es fundamental destacar que durante esta fase no se realiza ninguna evaluación de seguridad real; mas bien se trata de un periodo dedicado exclusivamente a la preparación y organización meticulosa de la prueba venidera.
- Fase de Descubrimiento: Durante esta etapa, implica una exploración exhaustiva y recolección de datos sobre la infraestructura tecnológica de la organización. Además, se realizan escaneos parea identificar servicios activos y tecnológicos; con esta información se procede a buscar posibles vulnerabilidades, consultando tanto bases de datos públicas como propias.
- Fase de Ejecución: Esta fase representa el núcleo de todo el proceso. Se pone a prueba las vulnerabilidades identificadas anteriormente, intentando explotarlas. Cuando un ataque resulta exitoso, se procede a aislar y docuemntar detalladamente la

vulnerabilidad, además de sugerir medidas para corregirla. Las actividades durante esta fase incluyen la obtención y escalada de privilegios, así como la exploración interna del sistema. En ocasiones, puede ser necesario instalar herramientas adicionales para recopilar más información o conseguir accesos de mayor nivel.

- Fase de Documentación y Reporte: Esta fase se desarrolla en paralelo con las etapas anteriores y se encarga de la recopilación de información para el reporte final. En la fase de Planificación, se documentan las reglas de evaluación y las pautas de interacción. En la fase de Descubrimiento, se almacenan los informes generados por los escáneres de vulnerabilidades y otra información relevante obtenida. En la fase de Ejecución, se conservan los informes generados por las herramientas de explotación de vulnerabilidades. Al finalizar la prueba de intrusión, se crea un informe que describe las vulnerabilidades identificadas, proporciona una calificación de riesgos y ofrece recomendaciones para mitigar las debilidades encontradas.

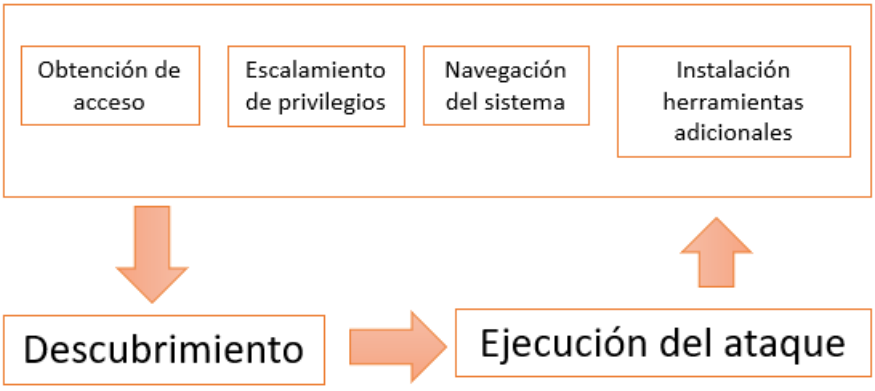


Figura 3 Actividades específicas de la Fase de Ejecución.

Fase de Análisis:

La NIST SP 800-115 proporciona una guía general para llevar a cabo un proceso de Evaluación de Seguridad de la Información en una entidad, centrándose en la verificación de

aspectos técnicos en sistemas informáticos y redes de datos. Entre los aspectos más notables de esta guía se incluyen:

- Enfatiza la importancia de llevar a cabo todo el proceso como parte de un proyecto estándar, aplicando las metodologías de gestión correspondientes.
- Destaca la necesidad de definir claramente el alcance, los objetivos, las limitaciones, los roles y otros componentes para que todas las partes involucradas comprendan los resultados, posibles impactos y las medidas de mitigación, asegurando que el proceso de Evaluación de Seguridad de la Información no tenga un impacto negativo en el funcionamiento de la entidad más allá de lo permitido.
- Propone la creación de un documento fundamental llamado "Reglas de Interacción" (Rules of Engagement) que debe ser firmado por todas las partes involucradas.

Sin embargo, la NIST SP 800-115 no pretende ser la guía definitiva o la metodología completa para llevar a cabo Evaluaciones de Seguridad de la Información. Reconoce sus limitaciones y remite a otros documentos y metodologías que pueden ayudar a abordarlas. Las limitaciones más significativas incluyen:

- La descripción de las actividades y procesos es general y requiere adaptación a las condiciones y requisitos específicos de la entidad y el proceso de pruebas. No se proporcionan herramientas, pruebas de seguridad ni métodos específicos para cada fase.
- Reconoce la creciente amenaza de ataques contra aplicaciones, como las aplicaciones web, y considera que las evaluaciones de seguridad a nivel de aplicaciones son complejas y requieren múltiples técnicas y métodos. Por lo tanto, la guía no es adecuada para su uso independiente en pruebas de seguridad en aplicaciones web.

2.3. Marco legal

En Ecuador, la seguridad de la información en el ámbito de las telecomunicaciones está sujeta a un marco legal y regulatorio.

Ley Orgánica de Telecomunicaciones: Esta ley establece el marco general para la provisión de redes y servicios de telecomunicaciones. En su artículo 22, menciona la obligación de los operadores de garantizar el secreto e inviolabilidad de las comunicaciones (ECUADOR, 2015)

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: Esta ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas (NACIONAL, 2002)

Ley Orgánica de Protección de Datos Personales: Promulgada en 2021, esta ley establece el marco regulatorio para la protección de los datos personales, incluyendo su tratamiento, intercambio y almacenamiento (Asamblea-Nacional-Del-Ecuador, 2021).

Acuerdo Ministerial 025-2019 del Ministerio de Telecomunicaciones y de la Sociedad de la Información: Este acuerdo establece la Política de Seguridad de la Información para entidades de la Administración Pública Central, Institucional y dependientes de la Función Ejecutiva, que, si bien no aplica directamente a ISPs privados, establece estándares que pueden ser considerados como buenas prácticas en el sector (TELECOMUNICACIONES, 2019).

Resoluciones de la Agencia de Regulación y Control de las Telecomunicaciones ARCOTEL: Como ente regulador, ARCOTEL emite resoluciones que afectan directamente a los ISPs, incluyendo aspectos de seguridad de la información. Por ejemplo, la Resolución

ARCOTEL-2020-0473 establece normas de calidad para la prestación del servicio de acceso a internet (TELECOMUNICACIONES L. A., 2020) .

La Ley Orgánica de Comunicación establece disposiciones específicas relacionadas con la protección de datos y la privacidad de los usuarios de servicios de Internet (Asamblea-Nacional-Del-Ecuador, 2021).

Este marco teórico proporciona la base conceptual necesaria para comprender la importancia de la seguridad de los servidores de borde de ISP en AIRMAXTELECOM S.A. y las amenazas que enfrentan. Además, establece la relación entre la seguridad de la información, los servidores de borde de ISP y el marco legal y regulatorio en Ecuador.

CAPÍTULO III

MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

La investigación se llevó a cabo en las instalaciones de AIRMAXTELECOM S.A., ubicada en la ciudad de Ibarra en las direcciones Calixto Miranda y José Miguel Leoro. AIRMAXTELECOM S.A. cuenta con una infraestructura de red extensa que abarcaba algunas provincias del país, brindando servicios de conectividad a empresas y usuarios finales. El área de estudio se centró específicamente en las instalaciones y servidores de borde que componían la infraestructura de red de AIRMAXTELECOM S.A.

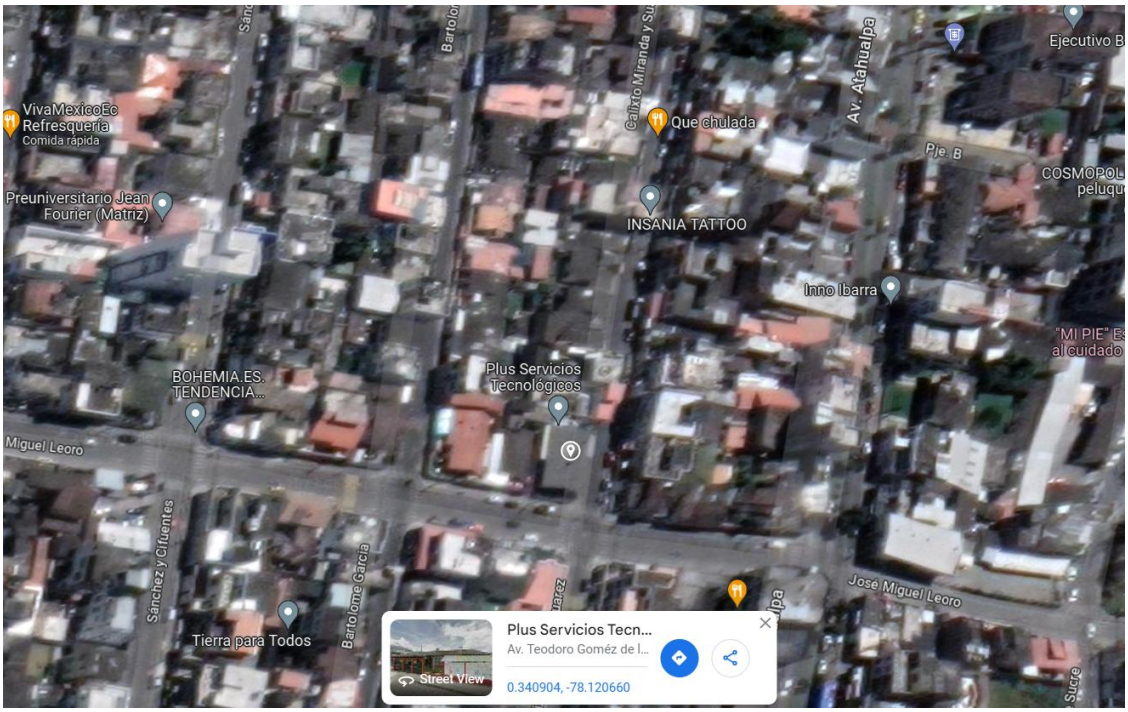


Figura 4 Ubicación de AIRMAXTELECOM S.A.

La elección de AIRMAXTELECOM S.A. como área de estudio se debió a su posición destacada en el sector de las telecomunicaciones en Ecuador y a la importancia crítica de garantizar la seguridad de sus servidores de borde. La empresa representó un caso de estudio ideal para evaluar la seguridad de los servidores de borde en un entorno operativo real y aplicar mejoras específicas basadas en los hallazgos.

El grupo de estudio en esta investigación estuvo compuesto por profesionales y expertos en seguridad de la información que trabajan en AIRMAXTELECOM S.A. Estos profesionales desempeñan roles clave en la planificación, implementación y supervisión de las medidas de seguridad de la información en la organización. Además, se incluyó un análisis exhaustivo de los servidores de borde de la empresa, que son esenciales en la infraestructura de red y eran puntos críticos para la seguridad de la información.

Los profesionales de seguridad de la información que participaron en el estudio cuentan con una amplia experiencia en el campo de la ciberseguridad y poseen conocimientos técnicos especializados relacionados con la configuración, protección y auditoría de los servidores de borde. Su participación en las entrevistas, así como en el análisis de documentos técnicos y políticas de seguridad, fue fundamental para comprender las prácticas de seguridad implementadas en ese momento y para identificar posibles áreas de mejora.

Este enfoque integral permitió una evaluación profunda de la postura de seguridad de AIRMAXTELECOM S.A., proporcionando perspectivas valiosas sobre las vulnerabilidades existentes y las oportunidades de fortalecimiento de la seguridad en los servidores de borde.

Los resultados de este estudio no solo benefician a la empresa en cuestión, sino que también sirve como lección aplicable a otras organizaciones del sector de las telecomunicaciones en Ecuador y más allá.

3.2. Enfoque y tipo de investigación

Esta investigación se enmarcó en un enfoque mixto que integró elementos cuantitativos y cualitativos. La elección de este enfoque se justificó por la naturaleza multidimensional de la problemática de seguridad en los servidores de borde de ISP en AIRMAXTELECOM S.A.

Enfoque Cuantitativo: Se utilizó para recopilar y analizar datos técnicos relacionados con la seguridad de los servidores de borde, incluyendo la identificación de vulnerabilidades y la evaluación de medidas de seguridad. Este enfoque implicó la medición de variables cuantitativas y el uso de análisis estadísticos para identificar patrones y tendencias.

Modelos de cuadros para el enfoque cuantitativo:

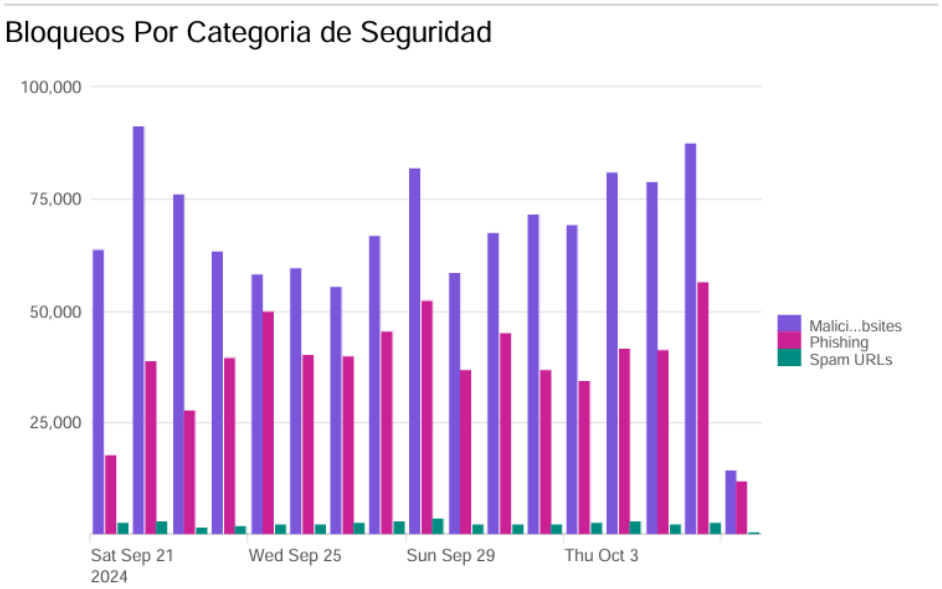


Figura 5 Bloqueos por categorías de seguridad
Fuente: AIRMAXTELECOM S.A.

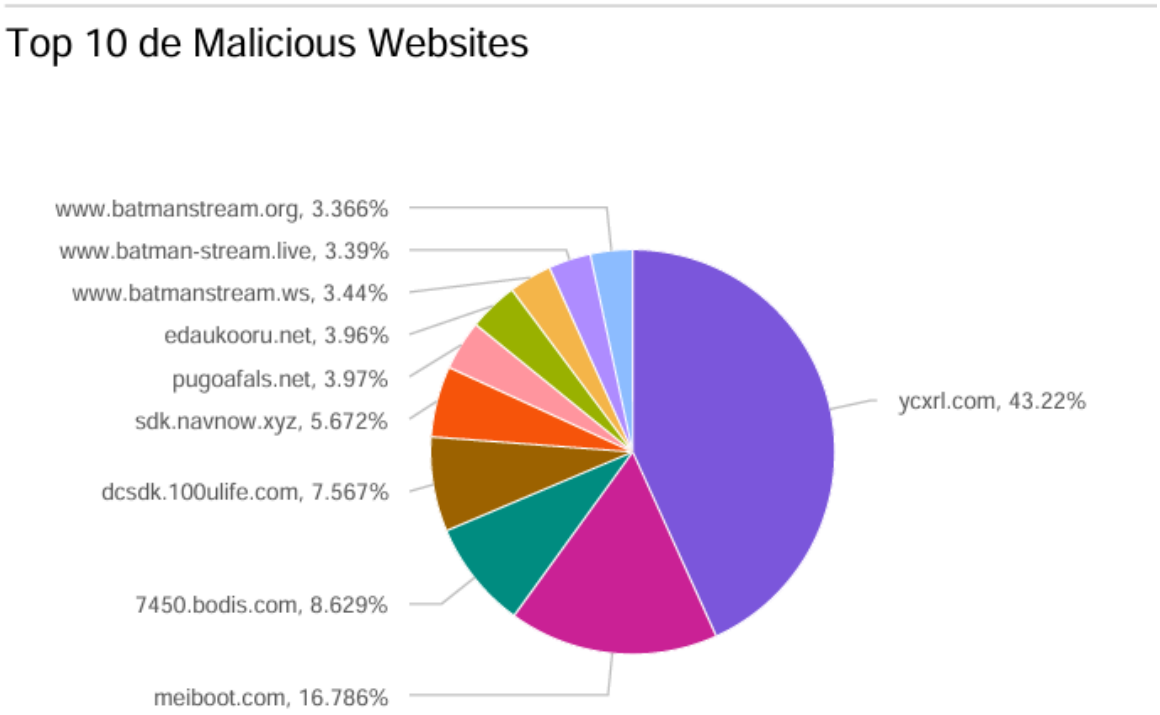


Figura 6 Páginas web maliciosas bloqueadas
Fuente: AIRMAXTELECOM S.A.

Enfoque Cualitativo: Se aplicó para explorar las percepciones, prácticas y desafíos relacionados con la seguridad de la información en AIRMAXTELECOM S.A. A través de entrevistas en profundidad, se obtuvo una comprensión más profunda de las experiencias de los profesionales de seguridad de la información y sus recomendaciones para mejorar la seguridad de los servidores de borde.

Fuentes de Información

Se analizaron políticas de seguridad, informes de incidentes, registros de acceso y datos técnicos proporcionados por AIRMAXTELECOM S.A., también se recopiló información mediante entrevistas en profundidad con profesionales de seguridad de la información y auditorías in situ de los servidores de borde.

Se buscó comprender la situación actual de la seguridad de los servidores de borde y explorar posibles áreas de mejora en un contexto poco estudiado.

Se describieron en detalle las prácticas existentes, los desafíos enfrentados y las vulnerabilidades identificadas.

Esta elección metodológica se ajustó a la necesidad de adentrarse en una problemática compleja y poco explorada, como es la seguridad de servidores de borde en el contexto de un ISP ecuatoriano. El uso de la guía NIST SP 800-115 proporcionó un marco estructurado para la evaluación, permitiendo una investigación rigurosa y alineada con estándares internacionales de seguridad de la información.

La investigación no solo describió el estado de la seguridad en AIRMAXTELECOM S.A., sino que también generó recomendaciones basadas en evidencia para mejorar la postura de seguridad de la empresa, contribuyendo así al conocimiento práctico en el campo de la ciberseguridad para ISPs en Ecuador y potencialmente en la región.

3.3. Procedimiento de la investigación

3.3.1. Fase1: Técnicas de identificación y análisis de objetivos

Esta fase, se detallan las metodologías empleadas para identificar y catalogar los activos de la red de AIRMAXTELECOM S.A. A través de técnicas de escaneo de puertos y servicios, se busca detectar dispositivos conectados y evaluar su estado de vulnerabilidad. Esta información inicial es fundamental para seleccionar los objetivos prioritarios de las pruebas de seguridad posteriores, alineadas con los lineamientos de la NIST SP 800-115.

3.3.1.1.Detección de redes

Utilizando herramientas como Nmap, Netdiscover en Kali linux, para identificar las redes disponibles y los dispositivos conectados a ellas.

El objetivo de la detección de redes es identificar los host o clientes finales que se encuentran en cada uno de los servidores para verificar si son vulnerables, para ello se procede a conectarse a la red local de cada uno de los servidores para identificar la subred dedicada a los clientes y posteriormente identificar todos los host o clientes activos para finalmente ver si son vulnerables.

Cuando se ejecuta el comando traceroute desde la consola de Kali, se está pidiendo a la computadora que rastree el camino que toman los datos desde tu computadora hasta el servidor DNS de Google (8.8.8.8), que es un servicio muy utilizado en Internet para convertir nombres de dominio en direcciones IP.

El comando traceroute muestra una lista de "saltos" o nodos que los datos atraviesan en su camino hacia el servidor DNS de Google. Cada línea en la lista representa un salto diferente en la red y en algún salto se identifica la subred dedicada a clientes finales

Con el comando netdiscover -i eth0, se está utilizando la herramienta Netdiscover en Kali Linux para descubrir dispositivos activos en la red local que pertenecen a la subred.

Netdiscover: Es una herramienta de escaneo de red que se utiliza para descubrir y enumerar dispositivos activos en una red local.

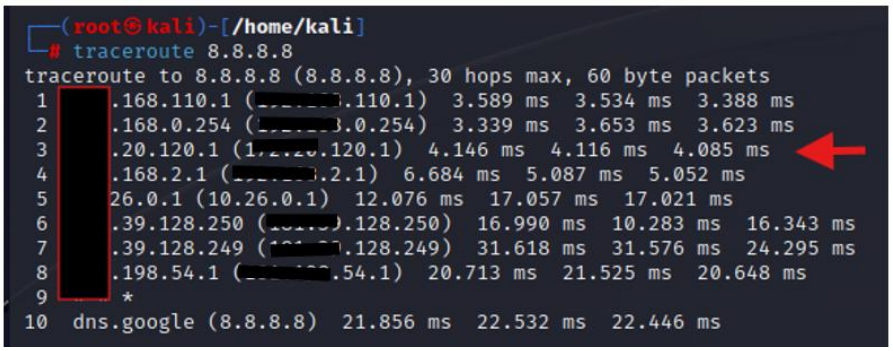
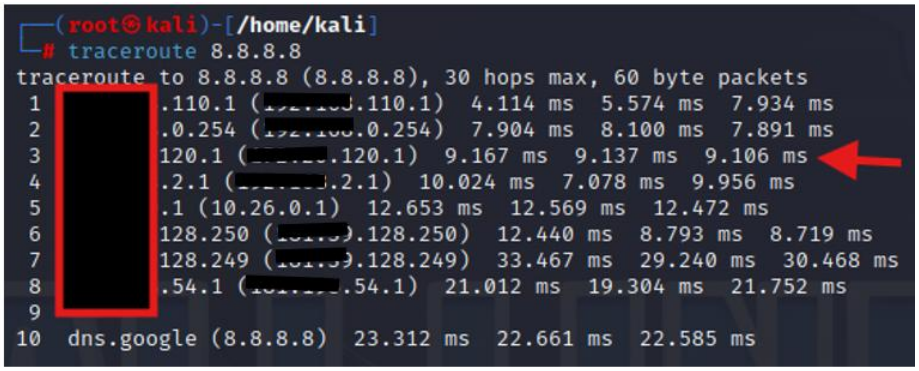
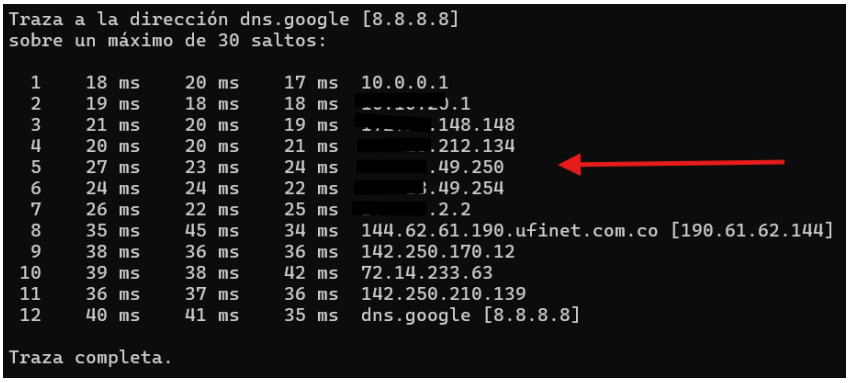
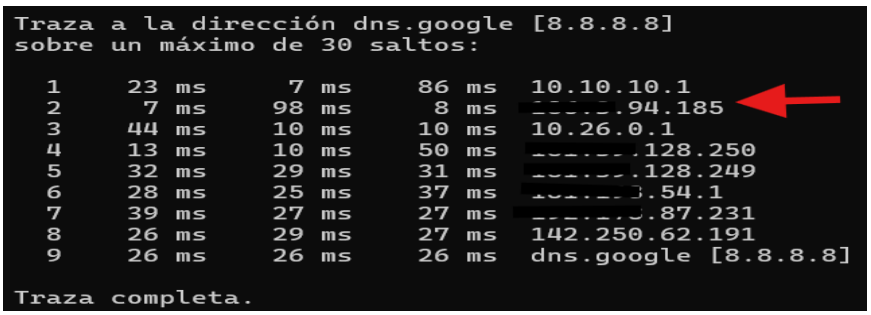
-i eth0: Esto especifica la interfaz de red que se utilizará para llevar a cabo el escaneo. En este caso, eth0 es el nombre de la interfaz de red en tu sistema. Puede ser diferente dependiendo de la configuración de tu sistema.

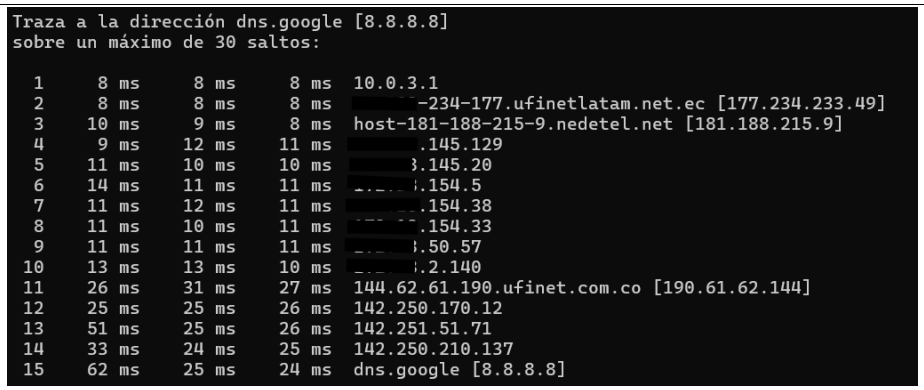
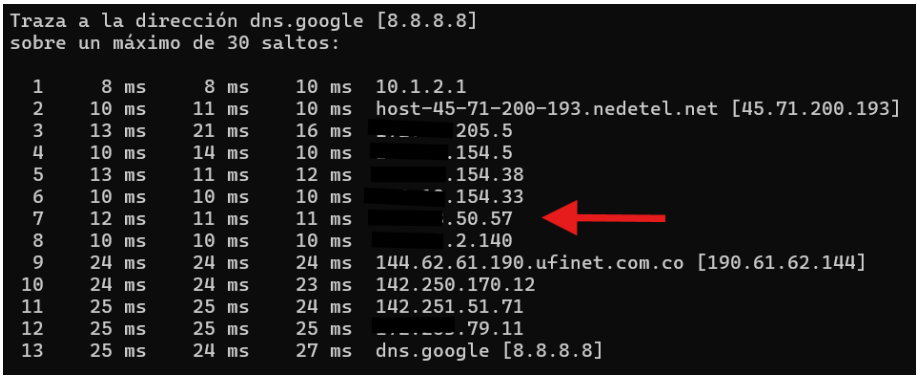
-r: Esta opción indica a Netdiscover que debe realizar el escaneo en la subred especificada.

Encontrando la subred por servidores

Tabla 1 ESCANEO DE PUERTOS DE LOS SERVIDORES

SEVIDOR	ESCANEO DE SUBRED
Ibarra	

	
Bolívar	
Pimampiro	
Urcuqui	
Cotacachi	

	
Otavalo	

Fuente: Autor

3.3.1.2.Identificación de puertos de red y servicios

Empleando herramientas de escaneo de puertos como Nmap para identificar qué puertos están abiertos en los dispositivos de la red y qué servicios están siendo ejecutados en esos puertos.

Trabajaremos en cada uno de los 6 servidores tratando de encontrar vulnerabilidades.

NMAP

Este comando **nmap -T4 -A -v** ejecuta un escaneo rápido y agresivo que intenta detectar los sistemas operativos y versiones de servicios en los hosts de la red, y proporciona una salida detallada del proceso. Es útil para obtener una visión general rápida pero detallada de los dispositivos y servicios en una red.

Servidor Ibarra

Este escaneo de Nmap muestra que varios puertos están filtrados, lo que significa que el escáner no pudo determinar si los puertos están abiertos o cerrados debido a la configuración de seguridad de los dispositivos o el firewall en la red. Los puertos que

están "filtered" incluyen los puertos típicos asociados con servicios como FTP (20/tcp, 21/tcp), SSH (22/tcp), Telnet (23/tcp), SMTP (25/tcp), SMB (135/tcp, 139/tcp, 445/tcp), entre otros.

Además, Nmap indica que hay demasiadas huellas digitales coincidentes para proporcionar detalles específicos sobre el sistema operativo del host escaneado. Esto sugiere que el host puede tener una configuración de seguridad que dificulta la identificación precisa del sistema operativo.

Servidor Bolívar

El resultado "179/tcp open tcp wrapped" indica que el puerto TCP 179 está abierto en el host escaneado, y está envuelto por TCP wrappers.

TCP wrappers es una herramienta de seguridad que controla el acceso a servicios de red basados en TCP mediante la configuración de un archivo llamado /etc/hosts.allow y /etc/hosts.deny. Cuando un servicio está envuelto por TCP wrappers, significa que las conexiones entrantes a ese servicio se filtran a través de las reglas definidas en estos archivos.

El hecho de que el puerto esté abierto y envuelto por TCP wrappers indica que el servicio asociado con el puerto 179 está disponible para conexiones entrantes, pero su acceso puede estar limitado o controlado por las reglas definidas en los archivos de configuración de TCP wrappers.

Servidor Pimampiro

Los puertos 20, 21, 22, 23, 25, 135 y 139 están marcados como "filtered". Esto significa que Nmap no pudo determinar si estos puertos están abiertos o cerrados debido a algún tipo de bloqueo, posiblemente por un firewall u otro dispositivo de seguridad.

El puerto 443 está marcado como "abierto", lo que significa que el servicio asociado (en este caso, HTTPS) está disponible y respondiendo a las solicitudes de conexión.

La máquina escaneada probablemente esté protegida por un firewall o algún otro mecanismo de seguridad que bloquea el acceso a la mayoría de los puertos, excepto al puerto 443 que está abierto y acepta conexiones SSL/HTTPS.

Servidor Urcuqui

Los resultados indican que la mayoría de los servicios comunes están bloqueados o no están respondiendo, mientras que hay un servidor MikroTik de prueba de ancho de banda abierto en el puerto 2000. El estado "filtrado" sugiere que estos puertos están protegidos por algún tipo de seguridad o están configurados para no responder a solicitudes de escaneo.

Servidor Cotacachi

La mayoría de los servicios comunes están bloqueados o no están respondiendo a las solicitudes de escaneo, excepto el puerto 443 que está abierto y acepta conexiones SSL/HTTPS.

Servidor Otavalo

La mayoría de los servicios comunes están bloqueados o no están respondiendo a las solicitudes de escaneo, excepto el puerto 443 que está abierto y acepta conexiones SSL/HTTPS. Esto sugiere que el servidor tiene al menos un servicio web seguro en funcionamiento.

3.3.1.3.Análisis de vulnerabilidades

Utilizando herramientas de análisis de vulnerabilidades como Nessus y Metasploit para identificar posibles vulnerabilidades en los servicios y sistemas encontrados durante el escaneo de la red.

Nessus es una herramienta de seguridad ampliamente reconocida que se utiliza para identificar y evaluar posibles debilidades en redes, sistemas y aplicaciones. Con Nessus, los expertos en seguridad pueden realizar análisis detallados para descubrir puertos abiertos, detectar vulnerabilidades y evaluar la configuración de seguridad. Además, la herramienta ofrece capacidades de análisis de cumplimiento y detección de malware. Una vez completado el escaneo, Nessus genera informes detallados que destacan las vulnerabilidades encontradas y proporciona recomendaciones para mitigar el riesgo. En resumen, Nessus es una herramienta esencial para mejorar la postura de seguridad de cualquier entorno de red, sistema o aplicación.

Servidor Ibarra

El informe de Nessus para el escaneo de la dirección IP del servidor muestra una variedad de vulnerabilidades y detalles de configuración del sistema.

Vulnerabilidades totales: El escaneo identificó un total de 26 hallazgos, que incluyen tanto vulnerabilidades como información sobre la configuración del sistema.

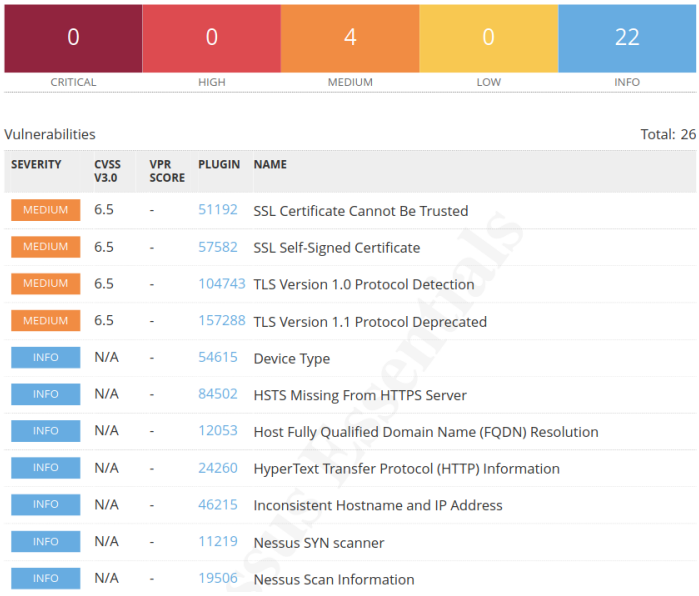
Gravedad de las vulnerabilidades: Se detectaron cuatro vulnerabilidades de severidad media, todas relacionadas con problemas en la configuración de SSL/TLS y protocolos obsoletos.

Las vulnerabilidades de gravedad media están relacionadas con certificados SSL no confiables, certificados autofirmados, detección de protocolos TLS obsoletos y la falta de soporte para HSTS (HTTP Strict Transport Security).

La mayoría de los hallazgos INFO proporcionan información sobre el entorno escaneado, incluyendo detalles sobre el tipo de dispositivo, resolución de nombres de host, información de HTTP, información de SSL/TLS, y detalles de detección de servicios y protocolos.

Se detectaron varias configuraciones relacionadas con SSL/TLS, incluidas las suites de cifrado admitidas, información sobre los certificados SSL, y detalles sobre los protocolos y suites de cifrado compatibles.

También se encontró información sobre la detección de servicios y protocolos, como versiones de TLS, servicios desconocidos y archivos "robots.txt" que podrían exponer información del servidor web.



0	0	4	0	22
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 26

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	-	54615	Device Type
INFO	N/A	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information

Figura 7 Análisis Vulnerabilidades - Servidor Ibarra
Fuente: Autor

Servidor Bolívar

El informe de Nessus para este escaneo muestra tres hallazgos, todos ellos clasificados como información (INFO), lo que indica que no representan vulnerabilidades críticas, altas, medias o bajas, sino que proporcionan detalles sobre el proceso de escaneo y precauciones recomendadas.

INFO N/A - 44920 Do not scan printers (AppSocket): Este hallazgo advierte sobre la no necesidad de escanear impresoras que utilizan el protocolo AppSocket. Esta precaución se basa en que el escaneo de impresoras sin una necesidad específica puede ser una práctica riesgosa y no recomendada.

INFO N/A - 11219 Nessus SYN scanner: Indica que Nessus utilizó el escáner SYN durante el escaneo. Esta es solo una información sobre la herramienta utilizada para realizar el escaneo.

INFO N/A - 19506 Nessus Scan Information: Proporciona información general sobre el escaneo realizado por Nessus. Esto puede incluir detalles sobre el rango de direcciones IP escaneadas, la duración del escaneo, entre otros detalles relacionados con el proceso de escaneo.

Los hallazgos de este escaneo son principalmente informativos y proporcionan detalles sobre el proceso de escaneo, así como recomendaciones sobre precauciones específicas, como no escanear impresoras que utilizan el protocolo AppSocket. No se identificaron vulnerabilidades críticas, altas, medias o bajas en este informe.

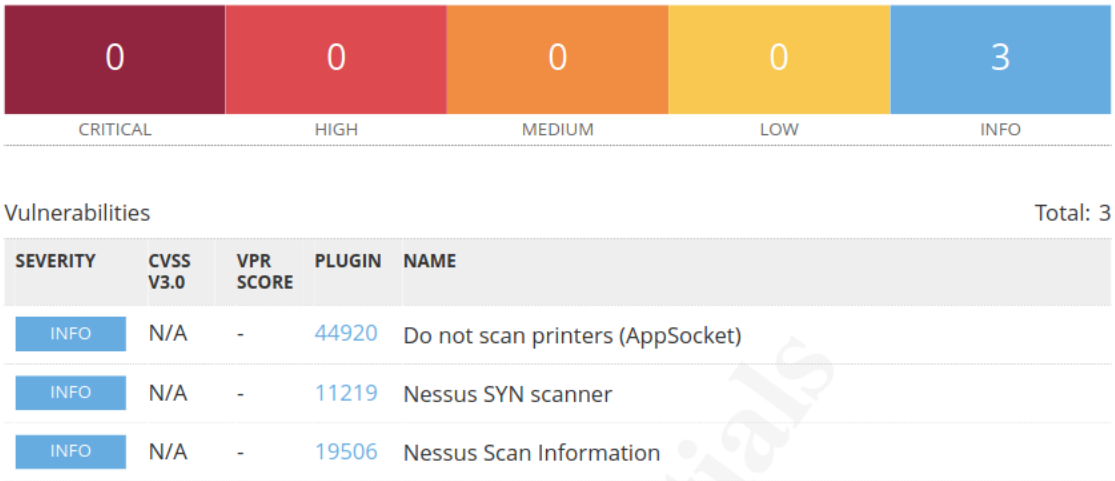


Figura 8 Análisis Vulnerabilidades - Servidor Bolívar
Fuente: Autor

Servidor Pimampiro

El informe de Nessus para este escaneo muestra diez hallazgos, todos clasificados como información (INFO), lo que indica que no representan vulnerabilidades críticas, altas, medias o bajas, sino que proporcionan detalles sobre el entorno escaneado.

INFO N/A - 54615 Device Type: Proporciona información sobre el tipo de dispositivo detectado durante el escaneo.

INFO N/A - 12053 Host Fully Qualified Domain Name (FQDN) Resolution: Indica si se pudo resolver correctamente el nombre de dominio completo (FQDN) del host escaneado.

INFO N/A - 24260 HyperText Transfer Protocol (HTTP) Information: Proporciona información sobre el protocolo HTTP y detalles relacionados con el servidor web.

INFO N/A - 46215 Inconsistent Hostname and IP Address: Indica si hay alguna inconsistencia entre el nombre de host y la dirección IP del host escaneado.

INFO N/A - 11219 Nessus SYN scanner: Indica que Nessus utilizó el escáner SYN durante el escaneo.

INFO N/A - 19506 Nessus Scan Information: Proporciona información general sobre el escaneo realizado por Nessus.

INFO N/A - 11936 OS Identification: Indica si Nessus pudo identificar el sistema operativo del host escaneado.

INFO N/A - 22964 Service Detection: Proporciona información sobre la detección de servicios en el host escaneado.

INFO N/A - 10287 Traceroute Information: Proporciona información sobre la ruta de red hacia el host escaneado.

INFO N/A - 10302 Web Server robots.txt Information Disclosure: Indica si se detectó alguna revelación de información en el archivo "robots.txt" del servidor web.

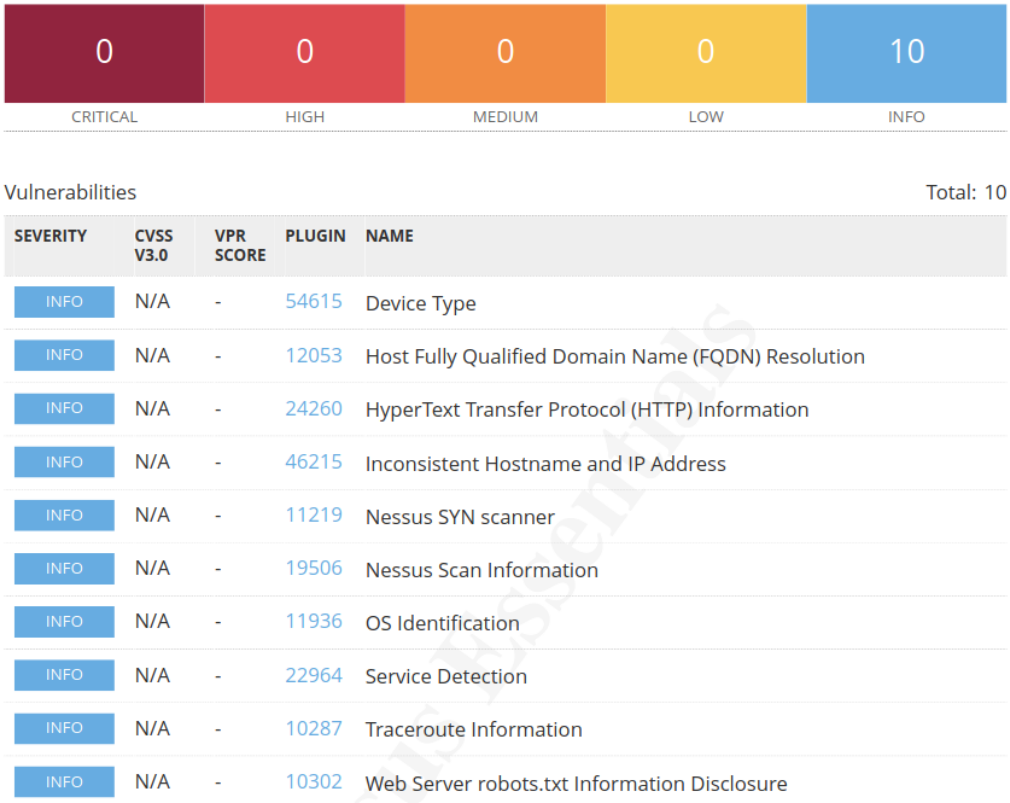


Figura 9 Análisis Vulnerabilidades - Servidor Pimampiro
Fuente: Autor

Servidor Urcuqui

El informe de Nessus para este escaneo muestra tres hallazgos, todos ellos clasificados como información (INFO), lo que indica que no representan vulnerabilidades críticas, altas, medias o bajas, sino que proporcionan detalles sobre el proceso de escaneo y precauciones recomendadas.

INFO N/A - 44920 Do not scan printers (AppSocket): Este hallazgo proporciona una advertencia sobre no escanear impresoras que utilizan el protocolo AppSocket. Esto es importante porque escanear impresoras sin una necesidad específica puede ser una práctica riesgosa y no recomendada.

INFO N/A - 11219 Nessus SYN scanner: Indica que Nessus utilizó el escáner SYN durante el escaneo. Esta es solo una información sobre la herramienta utilizada para realizar el escaneo.

INFO N/A - 19506 Nessus Scan Information: Proporciona información general sobre el escaneo realizado por Nessus. Esto puede incluir detalles sobre el rango de direcciones IP escaneadas, la duración del escaneo, entre otros detalles relacionados con el proceso de escaneo.

Los hallazgos de este escaneo son principalmente informativos y proporcionan detalles sobre el proceso de escaneo, así como recomendaciones sobre precauciones específicas, como no escanear impresoras que utilizan el protocolo AppSocket. No se identificaron vulnerabilidades críticas, altas, medias o bajas en este informe.

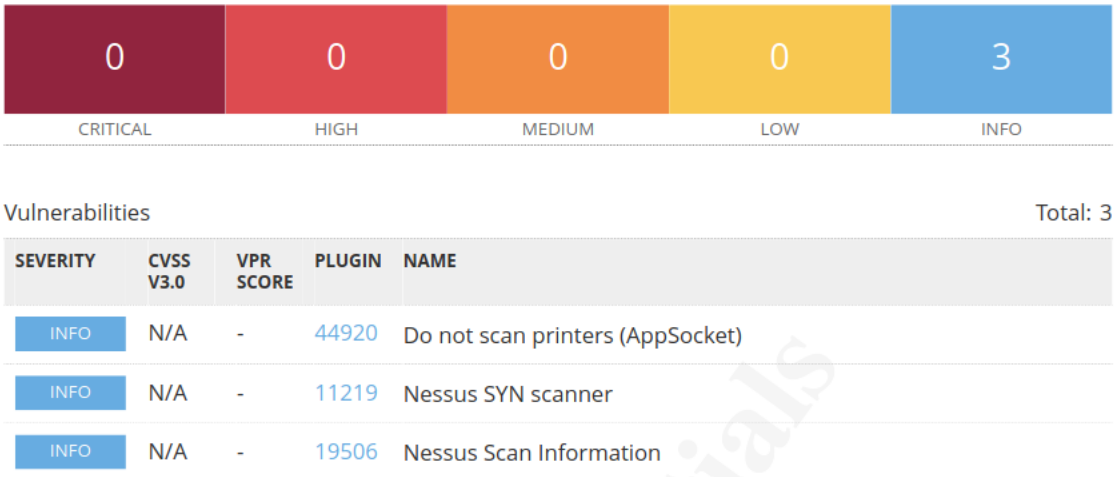


Figura 10 Análisis Vulnerabilidades - Servidor Urcuqui
Fuente: Autor

Servidor Cotacachi

El informe de Nessus para este escaneo muestra tres hallazgos, todos clasificados como información (INFO), lo que significa que no representan vulnerabilidades críticas, altas, medias o bajas, sino que proporcionan detalles sobre el proceso de escaneo y precauciones recomendadas.

INFO N/A - 44920 Do not scan printers (AppSocket): Este hallazgo indica que Nessus recomienda no escanear impresoras que utilizan el protocolo AppSocket. Escanear impresoras sin una necesidad específica puede ser riesgoso y no recomendado, ya que podría interferir con su funcionamiento normal.

INFO N/A - 11219 Nessus SYN scanner: Este hallazgo simplemente informa que Nessus utilizó su escáner SYN durante el proceso de escaneo. No indica ninguna vulnerabilidad o problema específico, solo proporciona información sobre la herramienta utilizada.

INFO N/A - 19506 Nessus Scan Information: Proporciona información general sobre el escaneo realizado por Nessus. Esto puede incluir detalles sobre el rango de direcciones IP escaneadas, la duración del escaneo y otros datos relevantes sobre el proceso de escaneo.

Estos hallazgos son informativos y proporcionan detalles sobre el proceso de escaneo y recomendaciones sobre precauciones específicas, como evitar escanear impresoras que utilizan el protocolo AppSocket. No se identificaron vulnerabilidades críticas, altas, medias o bajas en este informe.

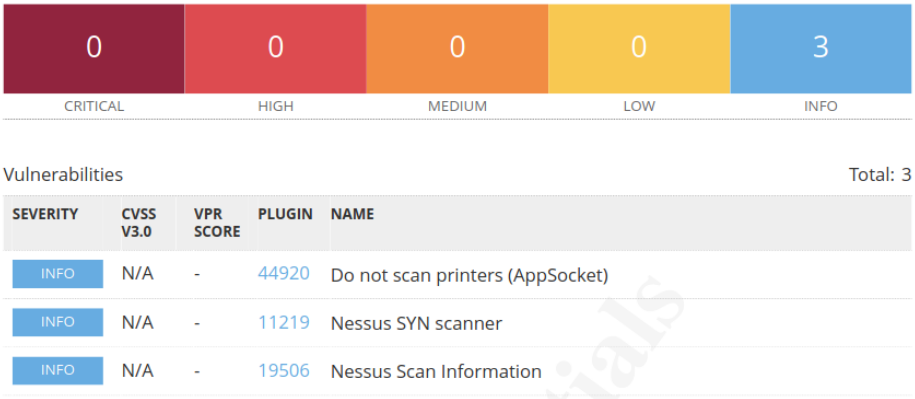


Figura 11 Análisis Vulnerabilidades - Servidor Cotacachi

Fuente: Autor

Servidor Otavalo

El escaneo de vulnerabilidades realizado por Nessus ha encontrado tres resultados, todos ellos clasificados como información (INFO), lo que significa que no representan una amenaza en sí mismos, pero proporcionan detalles sobre el entorno escaneado.

INFO N/A - 44920 Do not scan printers (AppSocket): Este resultado indica que Nessus ha detectado un servicio de impresión utilizando el protocolo AppSocket y sugiere que no escanees impresoras. Escanear impresoras sin una razón específica puede ser una práctica riesgosa y no recomendada.

INFO N/A - 11219 Nessus SYN scanner: Este resultado simplemente indica que se está utilizando el escáner SYN de Nessus para realizar el escaneo. No representa una vulnerabilidad en sí misma, sino más bien una parte del proceso de escaneo realizado por Nessus.

INFO N/A - 19506 Nessus Scan Information: Este resultado proporciona información general sobre el escaneo realizado por Nessus. Nuevamente, no representa una vulnerabilidad en el sistema escaneado, sino más bien detalles sobre la operación de escaneo realizada por Nessus.

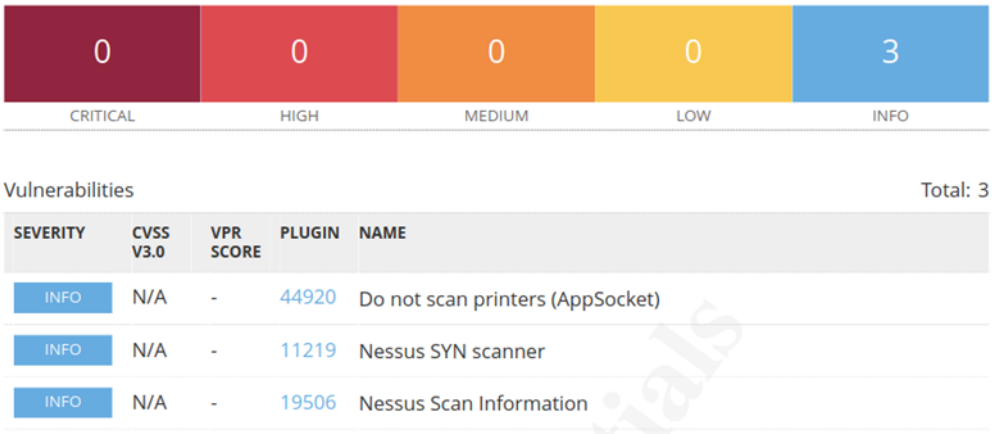


Figura 12 Análisis Vulnerabilidades - Servidor Otavalo
Fuente: Autor

Explotando vulnerabilidades con Metasploitable en los servidores

Existen exploits que pueden afectar a dispositivos MikroTik, como cualquier otro fabricante de equipos de red, ha experimentado vulnerabilidades de seguridad en el pasado, algunas de las cuales podrían ser aprovechadas mediante exploits para comprometer los dispositivos.

Algunos ejemplos de exploits efectivos para dispositivos MikroTik incluyen:

CVE-2018-14847: Este exploit afectó al servicio de gestión web (Winbox) de MikroTik RouterOS, permitiendo a un atacante no autenticado leer archivos arbitrarios en el sistema y ejecutar comandos remotos.

CVE-2019-3976: Este exploit afectó al servicio de gestión web (Winbox) y al servicio de configuración API de MikroTik RouterOS, permitiendo a un atacante no autenticado leer archivos arbitrarios en el sistema.

CVE-2020-5722: Este exploit afectó al protocolo de túnel SSTP (Secure Socket Tunneling Protocol) utilizado en MikroTik RouterOS, permitiendo a un atacante remoto enviar paquetes especialmente diseñados para provocar una denegación de servicio (DoS) o ejecutar código arbitrario.

Los tres exploits son efectivos únicamente en versiones de SO anteriores a la 6.4 y actualmente todos los servidores se encuentran actualizados el SO a la versión 7 o superior y los parches ya resuelven esta vulnerabilidad por lo que ninguno de los exploits es efectivo.

3.3.1.4.Escaneo inalámbrico activo y pasivo

Los servidores de borde MikroTik que forman parte de esta evaluación de seguridad están diseñados y configurados exclusivamente para funciones de red cableada. Estos dispositivos no incluyen módulos de conexión inalámbrica (Wi-Fi o Bluetooth) ni están integrados en redes que utilicen tecnología inalámbrica para su funcionamiento.

Ausencia de Interfaces Inalámbricas

Los servidores de borde MikroTik evaluados carecen de interfaces inalámbricas (Wi-Fi y Bluetooth). Esto significa que no emiten ni reciben tráfico inalámbrico, eliminando cualquier vector de ataque que pudiera aprovechar vulnerabilidades asociadas a redes inalámbricas.

Infraestructura de Red Cableada

La infraestructura de red de la empresa en la cual se implementan estos servidores de borde está basada completamente en conexiones cableadas. La seguridad y el monitoreo de la red se gestionan a través de estos enlaces físicos, y no se contempla la integración de redes inalámbricas en este segmento crítico de la infraestructura.

La metodología NIST SP 800-115 requiere una adaptación según los objetivos específicos y el contexto de la evaluación. En este caso, concentrar los recursos y esfuerzos en técnicas de detección y análisis pertinentes a redes cableadas (como la identificación de puertos y servicios, y el análisis de vulnerabilidades) resulta más eficiente y relevante.

Dado que los servidores de borde MikroTik no están equipados con tecnologías inalámbricas ni interactúan con redes inalámbricas, el escaneo inalámbrico no aporta valor en la identificación y mitigación de vulnerabilidades en este contexto específico.

En lugar de llevar a cabo técnicas de escaneo inalámbrico, se recomienda enfocar los esfuerzos en las áreas más relevantes y críticas para la seguridad de la red cableada

Al adaptar la metodología NIST SP 800-115 a las características específicas de los servidores de borde MikroTik, se asegura una evaluación de seguridad más precisa y efectiva, alineada con la infraestructura real y las necesidades de la empresa.

3.3.1.5.Resumen

Tabla 2 RESUMEN TÉCNICAS DE IDENTIFICACIÓN Y ANÁLISIS

Técnica	Capacidades	Detalles Técnicos
Detección de Redes	6 servidores analizados - Uso de Nmap y Netdiscover	- Comando traceroute - netdiscover -i eth0 - Identificación de subredes
Puertos y Servicios	- Ibarra: Múltiples puertos filtrados - Bolívar: Puerto 179 TCP wrapped - Pimampiro: Puerto 443 abierto - Urcuqui: Puerto 2000 (MikroTik) - Cotacachi: Puerto 443 - Otavalo: Puerto 443	- Nmap -T4 -A -v - Mayoría de puertos filtrados - HTTPS predominante
Análisis de Vulnerabilidades	- Ibarra: 26 hallazgos (4 medio) - Demás servidores: Solo INFO - Problemas SSL/TLS en Ibarra	- Herramientas: Nessus, Metasploit - Vulnerabilidades SSL - Certificados autofirmados
Redes Inalámbricas	- Sin interfaces Wireless - Solo conexiones cableadas - N/A para evaluación	- No hay Wi-Fi ni Bluetooth - Diseño exclusivo para red cableada

La evaluación de seguridad de los seis servidores de borde MikroTik muestra una infraestructura sólida y bien mantenida, con un enfoque claro en la seguridad de la red cableada. La eliminación de las interfaces inalámbricas y la elección de mantener estos servidores críticos solo en conexiones físicas demuestra una estrategia cautelosa para reducir la superficie de ataque. Los resultados muestran que la mayoría de los servidores tienen una postura de seguridad sólida, la mayoría de los puertos están filtrados adecuadamente y solo se muestran los servicios esenciales, principalmente HTTPS en el puerto 443.

3.3.2. Fase2: Vulnerabilidad de destino Técnicas de validación

Esta sección aborda las técnicas de validación de vulnerabilidades objetivo, utilizando la información obtenida a partir de la identificación y el análisis de objetivos para explorar más a fondo la existencia de vulnerabilidades potenciales. El objetivo es demostrar que existe una vulnerabilidad y exponer las posibles amenazas de seguridad que surgen cuando se explota. La validación de vulnerabilidades objetivo implica un mayor riesgo en las evaluaciones, ya que estas técnicas tienen más potencial para afectar al sistema o red de destino que otras técnicas.

3.3.2.1.Descifrado de Contraseñas

El descifrado de contraseñas en los servidores de borde MikroTik implica intentar recuperar las contraseñas utilizadas en estos dispositivos para identificar contraseñas débiles y mejorar la política de seguridad de la empresa AIRMAXTELECOM S.A. Este proceso puede descubrir credenciales inseguras que podrían ser explotadas por atacantes.

En la empresa AIRMAXTELECOM S.A. de servicios de internet, se utiliza servidores de borde de la marca MikroTik para gestionar el tráfico y garantizar la seguridad y eficiencia de la red. Estos dispositivos actúan como la primera línea de defensa y gestión, optimizando el enrutamiento y filtrado del tráfico entrante y saliente. Para la administración de estos servidores, se emplea Winbox, una herramienta gráfica que permite un acceso intuitivo y seguro a través de IP pública y credenciales de acceso específicas, asegurando que solo personal autorizado pueda realizar configuraciones y mantenimientos necesarios.

Identificación de los Hashes

Para la autenticación de usuarios hacia los servidores en MikroTik RouterOS, los algoritmos de hash más comunes son MD5 (especialmente en CHAP y MS-CHAP), y en algunos casos SHA-1 o SHA-256, dependiendo de la configuración específica del servidor RADIUS o del método de autenticación utilizado. Sin embargo, MD5 es el algoritmo de hash más frecuentemente empleado en estos contextos debido a su rapidez y compatibilidad, aunque no es el más seguro según los estándares actuales.

Ataques de diccionario de fuerza bruta

- Para ello necesario realizar un backup de cada uno de los servidores en la terminal de mikrotik con el comando /export file=backup, esto con el objetivo de encontrar los hashes de las contraseñas en los archivos de backup que se descargan en formato “rsc”.
- Como siguiente paso es encontrar los hashes en cada uno de los archivos descargados de los servidores para guardarlos en un archivo en formato “txt” como se muestra en la siguiente imagen.

- Ejecutar John the Ripper con cada uno de los archivos “txt” que almacenan los hashes de las contraseñas de acceso a los servidores para intentar descifrarlas.

  En la siguiente imagen se muestra una prueba didáctica con un hash de una contraseña simple y como se muestra en la siguiente imagen John the Ripper logra desencriptar:

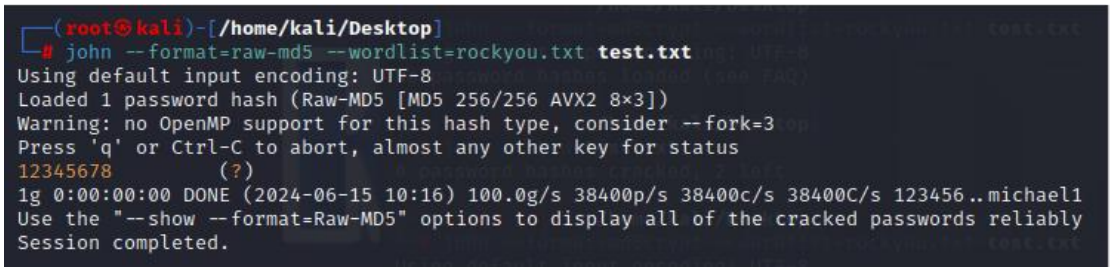


Figura 13 John The Ripper – Verificación de hash

Ahora probando con los hashes de los servidores se tiene los siguientes resultados, ninguna de las contraseñas ha podido ser desencriptada.

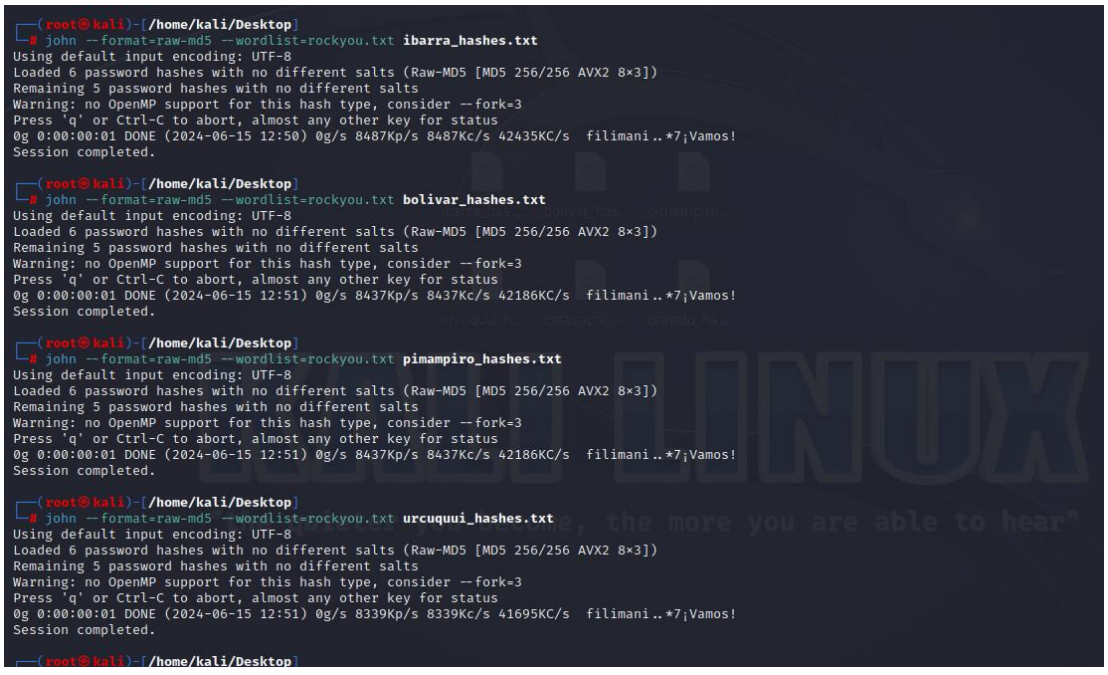


Figura 14 Jhon The Ripper - Sin exito en las contraseñas

Verificación de contraseñas descifradas:

A pesar de los intentos realizados, no se pudieron descifrar los hashes de las contraseñas de los servidores MikroTik. Esto indica que las contraseñas son suficientemente fuertes o no están presentes en la lista de palabras utilizada. Para

descifrar estas contraseñas, sería necesario un conjunto de herramientas y métodos más avanzados, o listas de palabras más específicas y extensas.

Los hashes en cuestión pertenecen a contraseñas de servidores de borde de los ISP de una empresa AIRMAXTELECOM.S.A. La infraestructura de red de un ISP es crítica y está sujeta a estrictas pruebas de este tipo de seguridad para garantizar la protección de los datos y la continuidad del servicio

A pesar de los esfuerzos realizados, no se pudieron descifrar los hashes de las contraseñas. Esto indica que las contraseñas utilizadas en los servidores MikroTik son suficientemente fuertes y seguras contra ataques de diccionario comunes, lo que refleja la efectividad de las políticas de seguridad implementadas.

3.3.2.2.Prueba de Penetración

En la empresa AIRMAXTELECOM S.A., se han identificado seis servidores de borde de la marca Mikrotik como objetivos para las pruebas de penetración. Estos servidores son críticos para la infraestructura de red de la empresa y su seguridad es fundamental para garantizar la continuidad y calidad del servicio proporcionado a los clientes.

Mikrotik es una marca conocida por sus dispositivos de red, incluyendo routers y switches, ampliamente utilizados en entornos empresariales. Sin embargo, como cualquier otro dispositivo de red, los equipos Mikrotik no están exentos de vulnerabilidades. Los Common Vulnerabilities and Exposures (CVE) son una lista de divulgaciones públicas de vulnerabilidades de seguridad. Algunas de las vulnerabilidades más comunes en los dispositivos Mikrotik incluyen:

CVE-2018-14847: Esta vulnerabilidad permite a un atacante remoto leer archivos arbitrarios desde el dispositivo afectado sin autenticación. Es explotable a través del puerto Winbox y se debe a una falla en la implementación de la autenticación en el servicio de administración Winbox.

3.3.2.2.1. Fases de prueba de penetración

Planeación

El objetivo principal de las pruebas de penetración en los servidores de borde Mikrotik de AIRMAXTELECOM S.A. es identificar y mitigar las vulnerabilidades de seguridad más comunes, específicamente aquellas documentadas como CVE, para asegurar la integridad, confidencialidad y disponibilidad de la red y los servicios ofrecidos.

Alcance

- Sistemas Objetivo: Seis servidores de borde Mikrotik en la red de AIRMAXTELECOM S.A.
- Tipos de Pruebas: Pruebas de caja negra, caja gris, y caja blanca, dependiendo del nivel de acceso permitido y la información proporcionada.
- CVE Objetivo: CVE-2018-14847 y otras vulnerabilidades comunes en dispositivos Mikrotik.

Reglas de Compromiso

- Equipos de prueba: Las pruebas se realizarán en servidores de prueba o copias realizadas de los servidores principales.
- Autorización: Se obtendrá autorización por escrito de la gerencia de AIRMAXTELECOM S.A. antes de iniciar cualquier prueba.
- Notificación: El equipo de TI y de seguridad de la empresa serán notificados antes, durante y después de las pruebas.

Actividades

- Identificar y documentar las versiones de firmware y configuraciones de los servidores Mikrotik.
- Recopilar información de red relevante, como rangos de IP, esquemas de subred, y rutas de tráfico.

Análisis de Vulnerabilidades:

- Identificar posibles vulnerabilidades utilizando bases de datos de CVE y escáneres de vulnerabilidades.

Pruebas de Explotación:

- Implementar y verificar la explotación del CVE-2018-14847 en un entorno controlado.
- Documentar el proceso de explotación y los resultados obtenidos.
- Intentar explotar otras vulnerabilidades comunes en Mikrotik, documentando todos los pasos y hallazgos.

Recolección de Evidencia:

- Mantener registros detallados de todas las actividades realizadas durante las pruebas.
- Capturar y guardar evidencia de cualquier acceso no autorizado obtenido, así como cualquier dato sensible.

Coordinación con las Partes Interesadas

- Equipo de TI: Colaborar estrechamente con el equipo de TI para asegurar una comprensión clara de la infraestructura de red y obtener apoyo técnico durante las pruebas.
- Seguridad de la Información: Trabajar con el equipo de seguridad para garantizar que las pruebas cumplan con las políticas y estándares de seguridad de la empresa.
- Gerencia: Mantener informada a la gerencia sobre el progreso de las pruebas y cualquier hallazgo crítico que requiera atención inmediata.

Descubrimiento

Se identifican seis servidores Mikrotik denominados PIMAMPIRO, BOLIVAR, IBARRA, URCUQUI, OTAVALO y COTACACHI, distribuidos en diversas ciudades del norte de Ecuador, cada uno funcionando como central de un ISP. La ubicación específica no se detalla por motivos de seguridad. Todos los servidores utilizan versiones de firmware superiores a la 7. Este inventario detalla los activos críticos que serán evaluados en las pruebas de penetración, enfocadas en garantizar la integridad, confidencialidad y disponibilidad de la red y servicios de AIRMAXTELECOM S.A.

Topología de red

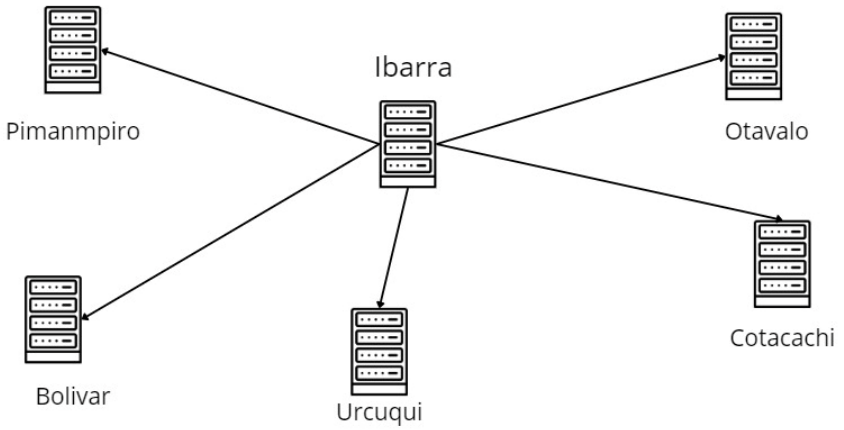


Figura 15 Topología de Red AIRMAXTELECOM S.A

AIRMAXTELECOM S.A. opera una red distribuida en el norte de Ecuador, utilizando servidores Mikrotik como puntos centrales de ISP en diferentes ciudades. Cada servidor Mikrotik tiene asignada una dirección IP pública única para permitir la conectividad desde y hacia Internet

Configuraciones de seguridad

- Se utiliza Winbox como principal herramienta de administración para acceder a los servidores Mikrotik.
- Los empleados tienen asignados usuarios únicos y credenciales individuales para iniciar sesión en Winbox, garantizando la trazabilidad y responsabilidad en las acciones administrativas realizadas.
- SSH está habilitado para permitir conexiones seguras y cifradas a los servidores Mikrotik desde ubicaciones externas.
- La configuración incluye la utilización de claves SSH para la autenticación, mejorando la seguridad del acceso remoto.
- Se permite el acceso a la interfaz web de los servidores Mikrotik para la gestión y configuración desde navegadores compatibles.
- El acceso web está protegido mediante HTTPS para cifrado de datos durante la transmisión y se controla mediante autenticación de usuarios.
- Se configuran reglas de firewall en los servidores Mikrotik para filtrar y controlar el tráfico entrante y saliente.

- Las reglas de firewall están diseñadas para permitir solo el tráfico esencial para las operaciones de red y servicios.
- Se implementa un sistema de auditoría y monitoreo para registrar y analizar las actividades administrativas y de acceso a los servidores Mikrotik.
- Se realizan revisiones periódicas de registros para detectar posibles anomalías o actividades sospechosas.

Ataque

La vulnerabilidad CVE-2018-14847, descubierta en el sistema operativo RouterOS de Mikrotik, ha tenido un impacto significativo en la seguridad de las redes que utilizan estos dispositivos. RouterOS es un sistema operativo y un software de router propietario que ofrece una amplia gama de funcionalidades, siendo muy popular en diversas implementaciones de redes debido a su flexibilidad y costo relativamente bajo.

Los routers de borde en los que se procederá el ataque se lo realiza desde una maquina Kali en donde se instala las funcionalidades y paquetes requeridos para aprovechar una de las vulnerabilidades más comunes como es CVE-2018-14847.

CVE-2018-14847 se clasifica como una vulnerabilidad crítica que permite a un atacante no autenticado leer archivos arbitrarios en un dispositivo Mikrotik. Esto se debe a una falla en la implementación del servicio de administración Winbox, que no maneja correctamente las solicitudes de acceso a los archivos del sistema.

La vulnerabilidad surge de la falta de validación adecuada en las peticiones que se realizan a través del servicio Winbox, permitiendo a un atacante remoto extraer archivos del sistema de archivos del dispositivo sin necesidad de autenticación. Entre los archivos que se pueden extraer, se incluyen aquellos que contienen las credenciales de administración del router, lo que puede llevar a una completa copromisión del dispositivo afectado.

El impacto de esta vulnerabilidad es considerable, ya que permite a un atacante obtener acceso privilegiado al dispositivo Mikrotik, acceder a la configuración del router, modificar reglas de firewall, redirigir tráfico, y potencialmente comprometer toda la red detrás del dispositivo afectado. Además, debido a la

naturaleza de la explotación, este tipo de ataques pueden realizarse de manera remota, lo que incrementa el riesgo y el alcance de la vulnerabilidad.

Ejecución del ataque

Para realizar el ataque necesitamos tener instalado Kali y acceder a la terminal como root, posteriormente actualizar los paquetes con el siguiente comando

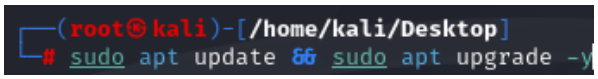


Figura 16 Actualización de Kali

Una vez actualizados paquetes, como punto importante es tener el router mikrotik de destino en la misma red y tener la dirección IP de este la cual será atacada.

Como siguiente paso es clonar el repositorio de git en donde se encuentra el código para explotar la vulnerabilidad con el siguiente comando.

Figura 17 Clonacion de repositorio

Para poder compilar el código en necesario tener instaladas las librerías y dependencias de Cmake y Boots que cumplen la siguiente función:

- CMake es una herramienta de automatización de compilación que gestiona el proceso de generación de sistemas de construcción multiplataforma. Proporciona una forma coherente de gestionar el proceso de compilación de proyectos, especialmente en entornos de desarrollo que utilizan múltiples compiladores y plataformas.

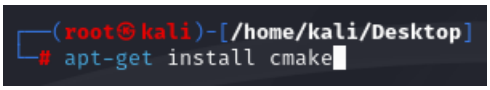


Figura 18 Instalación Cmake

- Boost es una colección de bibliotecas de C++ que amplían la funcionalidad del lenguaje estándar. Estas bibliotecas están diseñadas para ser portables y compatibles con los estándares de C++.

Figura 19 Instalación de Libboost

Como paso final para tener listo todo para intentar explotar la vulnerabilidad es compilara el código descargado con las siguientes líneas de comando.

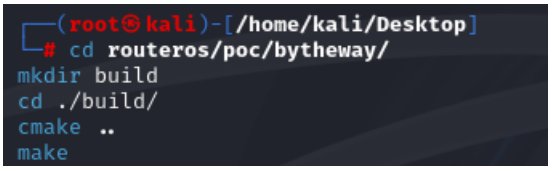


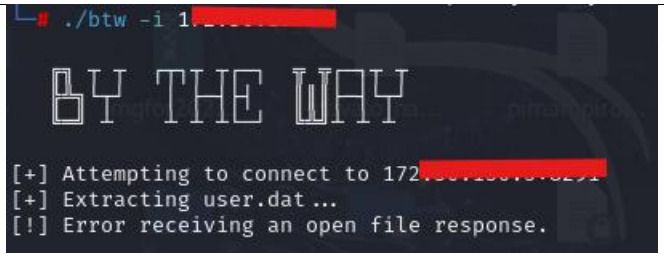
Figura 20 Compilación de códigos

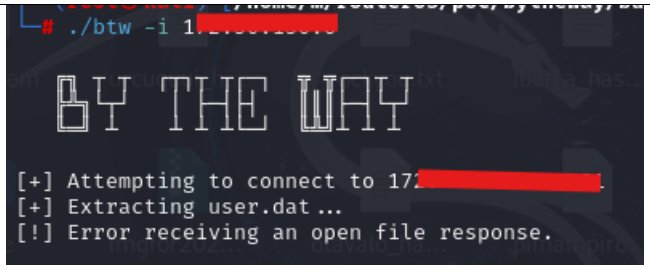
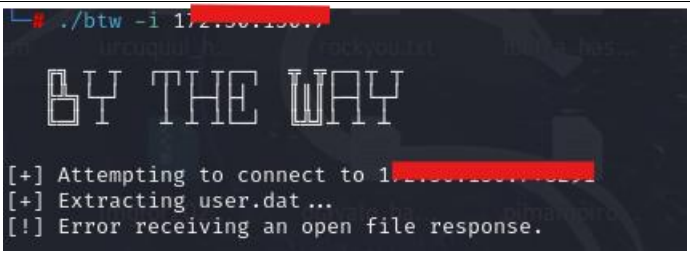
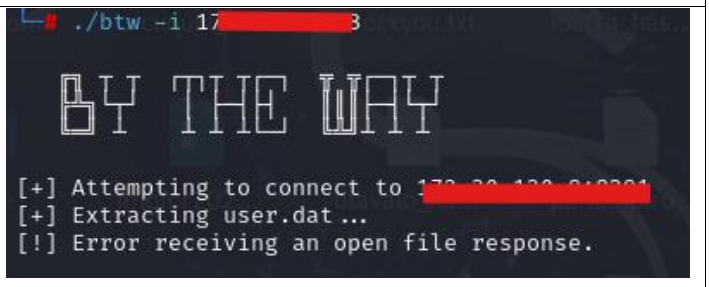
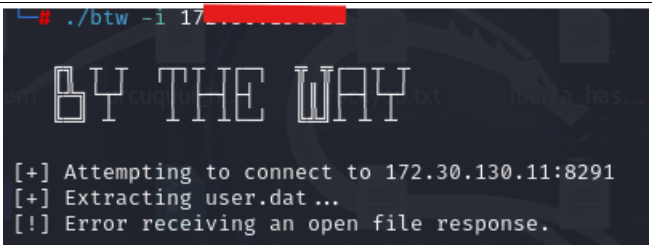
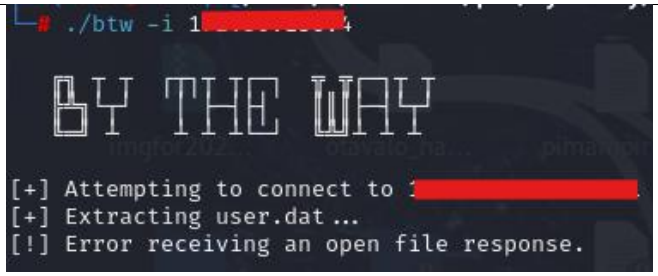
Antes de aplicar en los servidores reales es necesario verificar si hay comunicación entre la maquina atacante y el servidor objetivo con un simple ping.

En un caso ideal el exploit btw ejecutado debería mostrar las credenciales de acceso al servidor como se muestra en el siguiente ejemplo:

Figura 21 Ejemplo de credencial vulnerada

Tabla 3 PRUEBAS DE PENETRACION DE VULNERABILIDADES A SERVIDORES

SERVIDOR	PRUEBA DE EXPLOTACIÓN
Servidor Pimampiro	

Servidor Bolivar	
Servidor Ibarra	
Servidor Urcuqui	
Servidor Otavalo	
Servidor Cotacachi	

Informe

Se ha ejecutado el exploit btw en cada una de las direcciones IP de los servidores.

Esto indica que el exploit está intentando conectarse al dispositivo Mikrotik en la dirección IP de cuada uno de los servidores a través del puerto 8291, que es

el puerto predeterminado del servicio Winbox. Luego, intenta extraer el archivo user.dat, que normalmente contiene las credenciales de usuario del dispositivo.

[!] Error receiving an open file response

Este mensaje ha resultado ejecutando el exploit en cada uno de los servidores, esto indica que hubo un problema al intentar recibir una respuesta del dispositivo al abrir el archivo. Esto puede deberse a varias razones:

- El dispositivo puede no ser vulnerable: La versión de RouterOS que se está intentando atacar puede haber sido parcheada y no ser susceptible a la vulnerabilidad CVE-2018-14847.
- Problemas de conectividad: Puede haber problemas de red o de conectividad entre tu Kali Linux y el dispositivo Mikrotik cosa que no es congruente ya que se probó conexión antes de ejecutar el exploit.
- Restricciones de acceso: El dispositivo puede tener configuraciones de firewall u otras restricciones que están bloqueando el acceso al puerto 8291 o impidiendo la explotación a su vez cambiado el puerto por defecto de winbox

los resultados obtenidos sugieren que el dispositivo Mikrotik en cuestión es seguro frente a la vulnerabilidad CVE-2018-14847. No obstante, se recomienda mantener prácticas de seguridad proactivas para proteger el dispositivo contra futuras amenazas

3.3.2.2.2. Logística de pruebas de penetración

Herramientas Utilizadas: Nmap para escaneo de red, Metasploit para explotación de vulnerabilidades.

Medidas de Seguridad: Asegurarse de que las pruebas no afecten la operación normal de los servidores y que se realicen fuera de los horarios pico.

Validación Continua: Realizar pruebas periódicas para mantener la seguridad de los sistemas.

3.3.2.3.Ingeniería Social

Para evaluar la susceptibilidad de los empleados a ataques de ingeniería social, se ha optado por enfocarse específicamente en la técnica de phishing. El phishing

implica el envío de correos electrónicos fraudulentos diseñados para engañar a los destinatarios y hacer que revelen información confidencial, como credenciales de acceso. Este tipo de ataque es común y altamente efectivo, lo que lo convierte en un componente crucial de la evaluación.

Objetivo

Establecer los objetivos de la prueba de phishing, que pueden incluir:

- Evaluar la susceptibilidad de los empleados a ataques de phishing.
- Identificar áreas de mejora en la formación y concienciación sobre seguridad.
- Probar la efectividad de las políticas de seguridad existentes.

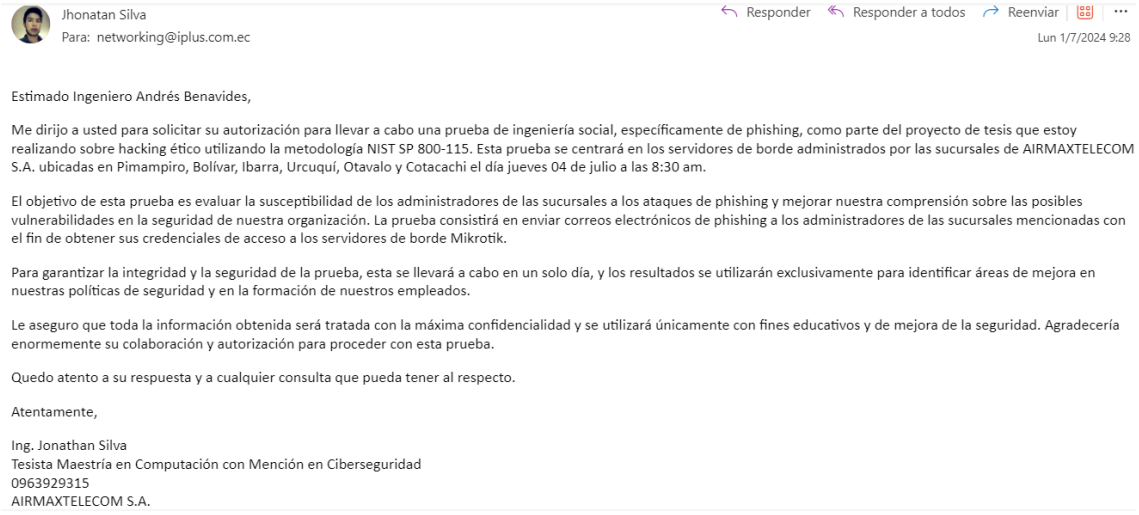
Alcance

La prueba de phishing se centrará en los administradores de las sucursales de la empresa ubicadas en seis ciudades diferentes, cada uno responsable de los servidores de borde Mikrotik de su respectiva sucursal. La prueba tendrá una duración de un día, durante el cual se enviarán correos electrónicos de phishing a los administradores con el objetivo de obtener sus credenciales de acceso a los servidores de borde Mikrotik.

Autorizaciones

- Permisos del jefe de networking y otros responsables relevantes.

Mediante correo electrónico se solicita autorización para llevar a cabo una prueba de ingeniería social a jefe de networking.



Jhonatan Silva
Para: networking@iplus.com.ec

Responder | Responder a todos | Reenviar | ...
Lun 1/7/2024 9:28

Estimado Ingeniero Andrés Benavides,

Me dirijo a usted para solicitar su autorización para llevar a cabo una prueba de ingeniería social, específicamente de phishing, como parte del proyecto de tesis que estoy realizando sobre hacking ético utilizando la metodología NIST SP 800-115. Esta prueba se centrará en los servidores de borde administrados por las sucursales de AIRMAXTELECOM S.A. ubicadas en Pimampiro, Bolívar, Ibarra, Urcuquí, Otavalo y Cotacachi el día jueves 04 de julio a las 8:30 am.

El objetivo de esta prueba es evaluar la susceptibilidad de los administradores de las sucursales a los ataques de phishing y mejorar nuestra comprensión sobre las posibles vulnerabilidades en la seguridad de nuestra organización. La prueba consistirá en enviar correos electrónicos de phishing a los administradores de las sucursales mencionadas con el fin de obtener sus credenciales de acceso a los servidores de borde Mikrotik.

Para garantizar la integridad y la seguridad de la prueba, esta se llevará a cabo en un solo día, y los resultados se utilizarán exclusivamente para identificar áreas de mejora en nuestras políticas de seguridad y en la formación de nuestros empleados.

Le aseguro que toda la información obtenida será tratada con la máxima confidencialidad y se utilizará únicamente con fines educativos y de mejora de la seguridad. Agradecería enormemente su colaboración y autorización para proceder con esta prueba.

Quedo atento a su respuesta y a cualquier consulta que pueda tener al respecto.

Atentamente,

Ing. Jonathan Silva
Tesista Maestría en Computación con Mención en Ciberseguridad
0963929315
AIRMAXTELECOM S.A.

Figura 22 Solicitud de autorización

Respuesta de jefe de Networking.

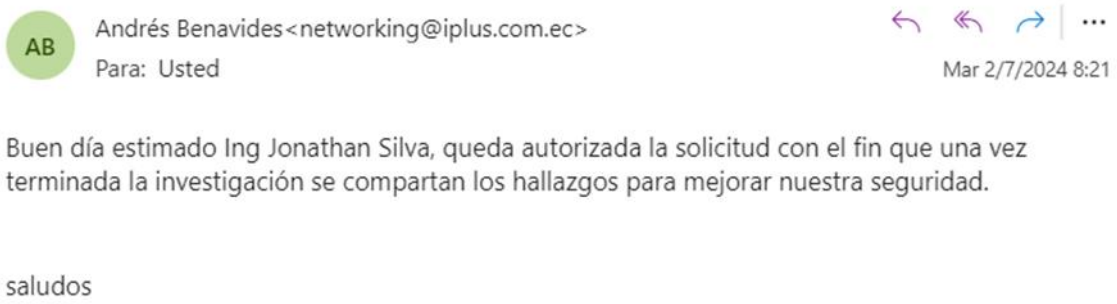


Figura 23 Aceptación de la solicitud

- Limitaciones y condiciones impuestas

  El jefe de networking no ha puesto ninguna limitación, ya que hay un compromiso de tratar la información obtenida con la máxima confidencialidad y se utilizará únicamente con fines educativos y la mejora de la seguridad de la empresa AIRMAXTELECOM S.A., a su vez solicita que una vez terminada la investigación se comparta hallazgos para la mejora de la seguridad.

Preparación

- Creación una cuenta de correo electrónico que simule ser del jefe de departamento, para ello se ha usado Gmail para hacer más eficiente él ya que los correos electrónicos de la empresa AIRMAXTELECOM S.A. tiene registros MX con Google suit, además de poner de foto de perfil la imagen de todos los trabajadores que manejan correos electrónicos corporativos.
- Diseño y redacción del correo electrónico de phishing, asegurándose de que sea creíble y relevante, en su efecto se insertó una firma para mejor credibilidad.
    - Previamente se verifico que el dominio iplus.com.ec sea susceptible a spoofing y que pueda ser efectivo el phinshing con la herramienta spoofcheck de Kali.
    - Haciendo pruebas previas el correo llegaba al spam y lo detectaba como phishing como se muestra en la imagen esto debido a que el servidor de correo de la empresa tiene un registro mx en Google suit

asi adopta las seguridades de Google y evita mensajes maliciosos de correos externos a la compañía.

- Finalmente, después de algunas configuraciones en Gmail que consiste en hacer chats con correos de la empresa para así pasar el filtro se redacta el mensaje de ingeniería social y se envía a las sucursales esperando sea efectivo

- Definición los indicadores de éxito

  Para evaluar la efectividad de la campaña de phishing realizada como parte de la fase de validación de vulnerabilidades, se envian correos electrónicos a seis administradores de sucursales, solicitando sus credenciales bajo el pretexto de una petición del jefe de networking. Los indicadores de éxito definidos para esta campaña fueron los siguientes:

  - Tasa de Apertura del Correo: El objetivo es que al menos 5 de los 6 administradores (≥ 83%) abran el correo. Este indicador mide la efectividad del asunto y del contenido inicial del correo en captar la atención de los destinatarios.
  - Tasa de Respuesta al Correo: Se espera que al menos 3 de los 6 administradores (≥ 50%) respondan al correo proporcionando las credenciales solicitadas. Este indicador refleja la eficacia del contenido del correo para persuadir a los administradores de cumplir con la solicitud.
  - Tiempo de Respuesta: El objetivo es que la mayoría de las respuestas (≥ 3) se reciban dentro de las primeras 2 horas. Este indicador proporciona información sobre la rapidez con la que los administradores reaccionan a las solicitudes recibidas por correo.
  - Tasa de Reporte del Correo: Se espera que 1 o menos de los 6 administradores (≤ 17%) reporten el correo como sospechoso o phishing. Este indicador mide la conciencia de seguridad de los administradores y su capacidad para identificar correos electrónicos fraudulentos.

- **Descubrimiento**

  Recolección de Información

Identificación las estructuras organizativas y los jefes de departamento reales. La estructura organizativa de la empresa de servicios de internet está diseñada para garantizar una administración eficiente y descentralizada de sus operaciones. A continuación, se detalla la configuración de la organización y los roles clave involucrados:

Estructura Organizativa:

Matriz

Departamento Operativo y Networking: La sede principal se encuentra en la matriz Ibarra, donde está centralizado el departamento operativo y de networking. Este departamento es responsable de la gestión global de la red y las operaciones técnicas de la empresa.

Jefe de Networking: El jefe de networking está a cargo de supervisar y coordinar todas las actividades relacionadas con la red en la organización. Este rol incluye la planificación estratégica, la gestión de recursos y la implementación de políticas de seguridad.

Colaboradores de Planta Interna: Un equipo de colaboradores trabaja bajo la dirección del jefe de networking en la matriz, encargándose de tareas técnicas y operativas dentro de la infraestructura de red.

Sucursales

Cada ciudad donde la empresa tiene presencia cuenta con un administrador de sucursal. Este administrador es responsable de las operaciones diarias en su respectiva ubicación.

Administrador de Sucursal: Además de sus responsabilidades administrativas, cada administrador tiene la capacidad de gestionar la red local y el servidor de borde en su ciudad. Esto incluye la administración de usuarios, configuración de red y mantenimiento de los servidores.

Correos Corporativos:

Todos los administradores de sucursales manejan correos corporativos con el dominio iplus.com.ec. Estos correos son esenciales para la comunicación interna y el acceso a los sistemas de la empresa.

Plan de Ingeniería Social:

Para llevar a cabo el ataque de ingeniería social, se planea enviar correos electrónicos de phishing a los administradores de las sucursales. El objetivo es hacerse pasar por el jefe de networking y solicitar las credenciales de acceso a

los servidores de borde. Los correos se diseñarán para parecer comunicaciones legítimas provenientes de la matriz, utilizando el dominio corporativo para aumentar su credibilidad.

- **Creación del Escenario**

  Para que el escenario sea lo más real posible se enviará un correo a cada uno de los administradores de las sucursales un correo que tenga la siguiente información solicitando las credenciales de los servidores para el manejo de las contraseñas y credenciales seguras:

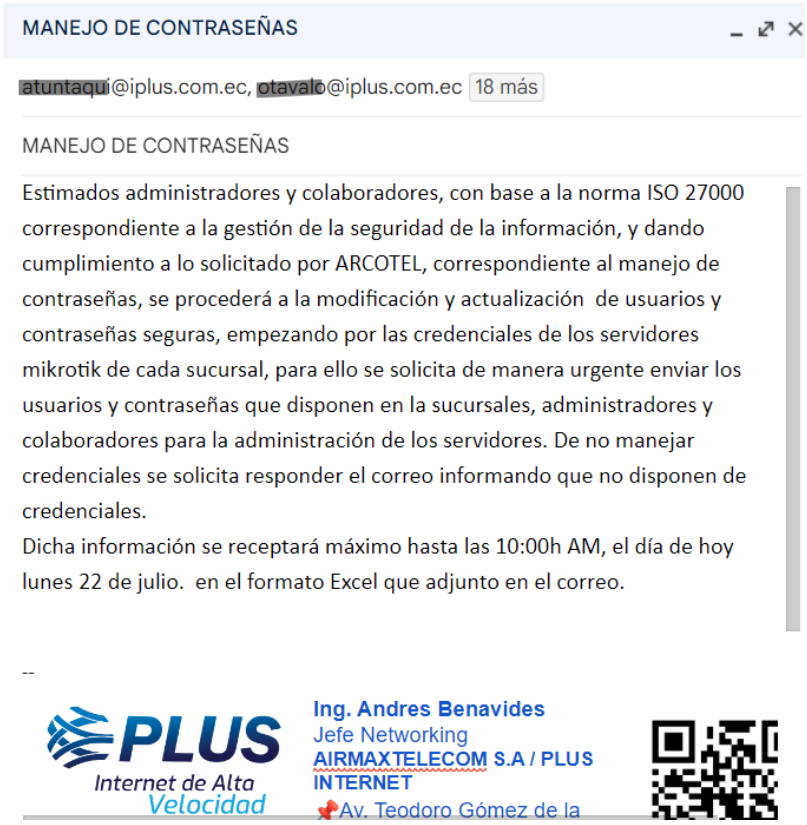


Figura 24 Email enviado a los usuarios

Ataque

Ejecución

Se redactó un correo electrónico simulando ser del jefe de networking, utilizando un tono formal y solicitando las credenciales de acceso a los servidores de borde.

El correo fue enviado desde una cuenta de Gmail configurada para parecer una comunicación legítima proveniente del dominio corporativo iplus.com.ec, incluyendo una firma creíble para aumentar su autenticidad.

Para el monitoreo de los correos se lo realiza con la herramienta mailtrack que se acopla a Gmail para darle seguimiento a los correos enviados, después de enviar los correos, se monitorearon las respuestas recibidas a través de la cuenta de Gmail utilizada para el phishing.

Registro de Resultados

Se enviaron un total de seis correos electrónicos, uno a cada administrador de las seis sucursales de AIRMAXTELECOM S.A.

De los seis correos enviados, se recibieron respuestas de seis administradores a pesar de que Gmail daba una advertencia de ser un correo de un usuario externo.

De las seis respuestas recibidas, tres administradores proporcionaron las credenciales completas de acceso a los servidores de borde.

Ninguno de los administradores ha solicitado confirmación adicional antes de compartir las credenciales completas.

Todos los administradores respondieron dentro de las primeras dos horas después de recibir el correo.

Análisis

Efectividad del Lenguaje y Urgencia del Mensaje:

El correo utilizo un lenguaje urgente y enfatizaron la necesidad inmediata de las credenciales, gracias a esto tuvo una tasa de respuesta alta.

La inclusión de detalles específicos sobre las operaciones de la empresa y la estructura organizativa aumentó la credibilidad del mensaje.

Susceptibilidad por Nivel Organizativo:

Los administradores con menos experiencia en seguridad informática fueron más propensos a proporcionar la información solicitada.

Aquellos con formación previa en concienciación sobre seguridad fueron más cautelosos y verificaron la legitimidad del correo antes de responder

Recomendaciones

- Implementar políticas más estrictas sobre la divulgación de credenciales y realizar verificaciones adicionales antes de compartir información sensible.
- Realizar sesiones de formación regulares para todos los empleados sobre cómo identificar correos electrónicos de phishing y otras amenazas de ingeniería social.
- Incluir simulaciones periódicas de phishing para evaluar y mejorar la capacidad de respuesta de los empleados ante tales amenazas.
- Implementar autenticación multifactor (MFA) para todos los accesos a los sistemas críticos.
- Mejorar los filtros de correo electrónico para detectar y marcar potenciales correos de phishing antes de que lleguen a los destinatarios.

3.3.2.4.Resumen

La metodología NIST SP 800-115 proporciona una guía estructurada para llevar a cabo pruebas de seguridad, incluyendo la planificación, descubrimiento, ataque y postataque. En el contexto de la empresa AIRMAXTELECOM S.A., se aplicaron estas fases para evaluar la seguridad de seis servidores de borde Mikrotik.

Fase de Planificación

Se definieron los objetivos y alcances de la prueba de seguridad, enfocándose en la recolección de credenciales de acceso mediante técnicas de ingeniería social, específicamente a través de correos de phishing. Se identificaron los administradores de las sucursales de la empresa como los objetivos principales.

Fase de Descubrimiento

Se recopiló información relevante sobre la infraestructura de red y los sistemas objetivo. Se utilizaron herramientas y técnicas para identificar posibles vulnerabilidades en los servidores Mikrotik, incluyendo la revisión de vulnerabilidades conocidas (CVE-2018-14847).

Fase de Ataque

Se ejecutaron pruebas de phishing enviando correos electrónicos diseñados para parecer comunicaciones legítimas de la matriz de la empresa. El objetivo era obtener credenciales de acceso a los servidores de borde. Los resultados mostraron que tres

de los seis administradores proporcionaron las credenciales completas sin solicitar confirmación adicional.

Fase de Postataque

Se validaron los resultados del ataque de phishing y se analizaron las contraseñas obtenidas. A pesar de los esfuerzos, no se pudieron descifrar los hashes de las contraseñas de los servidores MikroTik, lo que indica que son suficientemente fuertes. Se realizaron recomendaciones para mejorar la seguridad, incluyendo políticas más estrictas sobre la divulgación de credenciales, capacitación regular en seguridad informática y la implementación de autenticación multifactor.

Análisis y Recomendaciones

Contraseñas Descifradas

- Contraseñas simples deben evitarse.
- Contraseñas moderadamente complejas ofrecen seguridad mejorada, pero pueden mejorarse.
- Contraseñas altamente complejas son recomendables.

Pruebas de Penetración

- Verificación de vulnerabilidades y demostración de posibles explotaciones.
- Importancia de las políticas de seguridad y actualizaciones regulares de los sistemas.

Ingeniería Social

- Importancia de la concienciación del usuario respecto a la seguridad.
- Realización de simulaciones periódicas de phishing para evaluar la respuesta de los empleados.

3.3.3. Fase 3: Propuesta de Mejoras y Estrategias de Seguridad

Basándome en la metodología NIST SP 800-115 y en los resultados de la evaluación de seguridad realizada en los servidores de borde de AIRMAXTELECOM S.A., propongo las siguientes recomendaciones y estrategias para mejorar la seguridad:

Tabla 4 MEJORAS Y ESTRATEGIAS DE SEGURIDAD

Fase NIST SP 800-115	Categoría	Recomendación	Descripción
1. Planificación	**Objetivos y Alcance**	Definir objetivos de seguridad	Establecer metas claras para la protección de servidores de borde contra amenazas internas y externas.
		Determinar alcance de evaluaciones	Incluir todos los servidores MikroTik identificados en evaluaciones periódicas.
	Políticas y Procedimientos	Desarrollar política de seguridad	Crear una política integral específica para servidores de borde.
		Establecer procedimientos	Detallar procesos para gestión de accesos, actualizaciones y respuesta a incidentes.
	Recursos	Asignar personal especializado	Designar equipo dedicado a la gestión y monitoreo de seguridad de servidores.
		Presupuestar recursos	Asignar fondos para herramientas, capacitación y auditorías externas.
2. Descubrimiento	**Recopilación de Información**	Implementar gestión de activos	Mantener inventario actualizado de servidores de borde y sus caracterís-ticas.
		Realizar escaneos de red regulares	Usar Nmap para identificar cambios en topología o servicios expuestos.
	Análisis de Vulnerabilidades	Establecer programa de escaneo	Realizar escaneos periódicos con herramientas como Nessus.
		Priorizar resolución	Abordar vulnerabilidades según criticidad y contexto del negocio.
	Revisión de Configuraciones	Auditar configuraciones	Verificar cumplimiento con mejores prácticas de seguridad en servidores MikroTik.
		Implementar gestión de configuración	Mantener consistencia entre todos los servidores.
3. Ataque (Pruebas)	**Pruebas de Penetración**	Realizar pruebas anuales	Incluir ataques simulados contra servidores de borde.
		Probar vulnerabilidades específicas	Evaluar vulnerabilidades como CVE-2018-14847 en MikroTik.
	Evaluación de Controles	Probar efectividad de controles	Evaluar firewalls, IDS/IPS y mecanismos de autenticación.
		Evaluar respuesta a incidentes	Simular intrusiones para probar respuesta del equipo.

	Ingeniería Social	Simular phishing	Continuar y ampliar simulaciones de phishing.
		Mejorar procesos de respuesta	Refinar procedimientos basados en resultados de pruebas.
4. Post-Ataque	**Análisis de Resultados**	Analizar hallazgos	Examinar detalladamente resultados de pruebas y evaluaciones.
		Categorizar riesgos	Priorizar riesgos según impacto y probabilidad.
	Plan de Mitigación	Desarrollar plan detallado	Elaborar estrategias para abordar vulnerabilidades identificadas.
		Establecer plazos y responsables	Asignar tareas y fechas para implementación de medidas.
	Implementación de Mejoras	Fortalecer autenticación	Implementar MFA y reforzar políticas de contraseñas.
		Mejorar seguridad de red	Configurar firewalls y segmentación de red.
		Gestionar actualizaciones	Establecer proceso de actualización y gestión de parches.
		Implementar monitoreo	Desplegar IDS y logging centralizado.
		Realizar hardening	Asegurar servidores y usar protocolos seguros.
		Gestionar certificados	Usar certificados confiables y renovación automática.
	Capacitación	Desarrollar programa de capacitación	Entrenar personal en seguridad y concienciación.
		Realizar simulaciones	Ejecutar ejercicios de phishing y otros ataques.
	Mejora Continua	Revisar medidas periódicamente	Evaluar y adaptar estrategias de seguridad regularmente.
5. Documentación	**Elaboración de Informes**	Generar informes detallados	Documentar cada fase de evaluación de seguridad.
		Incluir métricas clave	Registrar y analizar evolución de métricas de seguridad.
	Comunicación	Presentar a dirección	Informar hallazgos y recomendaciones a alta gerencia.
		Proporcionar actualizaciones	Mantener informados a stakeholders sobre estado de seguridad.
	Mantenimiento de Registros	Mantener registro de actividades	Documentar todas las acciones de seguridad e incidentes.
		Cumplir requisitos legales	Asegurar que documentación cumpla normativas aplicables.

Estas recomendaciones se alinean con las mejores prácticas de seguridad de la información y la metodología NIST SP 800-115, abordando las vulnerabilidades identificadas en la evaluación y fortaleciendo la postura de seguridad general de los servidores de borde de AIRMAXTELECOM S.A.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

Este capítulo presenta los resultados y la discusión subsiguiente del testeo y evaluación de la seguridad de la información de los servidores de borde en la empresa AIRMAXTELECOM S.A., utilizando como marco de referencia la guía NIST SP 800-115. La investigación se centró en la identificación, análisis y mitigación de vulnerabilidades en la infraestructura crítica de red de este Proveedor de Servicios de Internet (ISP), con el objetivo de fortalecer su postura de seguridad.

Resultados de la Metodología Aplicada

La metodología NIST SP 800-115 proporcionó un enfoque estructurado para nuestra evaluación de seguridad, que se desarrolló en cuatro fases principales:

- **Fase de Planificación:** Se definieron los objetivos y el alcance de la prueba de seguridad, enfocándose en la recolección de credenciales de acceso mediante técnicas de ingeniería social, específicamente a través de correos de phishing. Los administradores de las sucursales fueron identificados como los objetivos principales. Con una tasa del 50% de éxito revela una vulnerabilidad considerable en los procedimientos de autenticación y concienciación sobre la seguridad de los servidores.
- **Fase de Descubrimiento:** Se recopiló información sobre la infraestructura de red y los sistemas objetivo. Se utilizaron herramientas como Nmap y Netdiscover para identificar posibles vulnerabilidades en los seis servidores Mikrotik analizados, incluyendo la revisión de vulnerabilidades conocidas como CVE-2018-14847. Además, el análisis reveló un entorno relativamente seguro con la mayoría de los puertos filtrados, excepto por los siguientes hallazgos notables:
    - Ibarra: Múltiples puertos filtrados, 26 vulnerabilidades detectadas (4 de severidad media).
    - Bolívar: El puerto 179 TCP se encontraba envuelto.
    - Pimampiro, Urcuqui, Cotacachi y Otavalo: Servicios HTTPS abiertos en el puerto 443.
- **Fase de Ataque**: El ataque de phishing dirigido tuvo éxito en el 50% de los casos. Los tres administradores afectados proporcionaron sus credenciales, lo que permitió un acceso potencial a los sistemas críticos. Sin embargo, no se logró descifrar los hashes de las contraseñas obtenidas, lo que evidencia la fortaleza de estas. A pesar de esto, la

facilidad con la que se obtuvieron las credenciales plantea un riesgo considerable para la seguridad de la red.

- **Fase de Postataque:** Después de validar los resultados, se realizó un análisis exhaustivo de las contraseñas. Las contraseñas no fueron descifradas, lo que sugiere que son suficientemente complejas. Sin embargo, se recomendó fortalecer las políticas internas para evitar la divulgación de credenciales mediante phishing, junto con la implementación de autenticación multifactor.

Discusión

Los resultados de la evaluación de seguridad indican que, a nivel de infraestructura, los servidores de borde Mikrotik están configurados de manera adecuada, con la mayoría de los puertos filtrados y una gestión eficaz de servicios críticos como HTTPS. No obstante, las vulnerabilidades identificadas en la configuración SSL/TLS del servidor en Ibarra son preocupantes, ya que el uso de certificados autofirmados y configuraciones incorrectas puede comprometer la seguridad de las comunicaciones en entornos externos.

El éxito parcial del ataque de phishing revela la necesidad urgente de mejorar la concienciación de seguridad entre los empleados. La obtención de credenciales mediante técnicas de ingeniería social demuestra que, aunque las contraseñas sean robustas, la seguridad de la infraestructura se ve comprometida por debilidades humanas. Este hallazgo subraya la importancia de llevar a cabo capacitaciones regulares sobre buenas prácticas de seguridad y la implementación de medidas como la autenticación multifactor para mitigar riesgos.

Finalmente, la decisión de mantener los servidores críticos en una red cableada y sin conexiones inalámbricas es un enfoque sólido que reduce la exposición a posibles ataques remotos, una estrategia adecuada para infraestructuras de misión crítica como la de AIRMAXTELECOM S.A.

En esta sección, se presentan los resultados detallados de la encuesta realizada al personal administrativo y técnico responsable de los servidores de AIRMAXTELECOM S.A. Esta encuesta fue diseñada para evaluar de la seguridad de la información en la empresa:

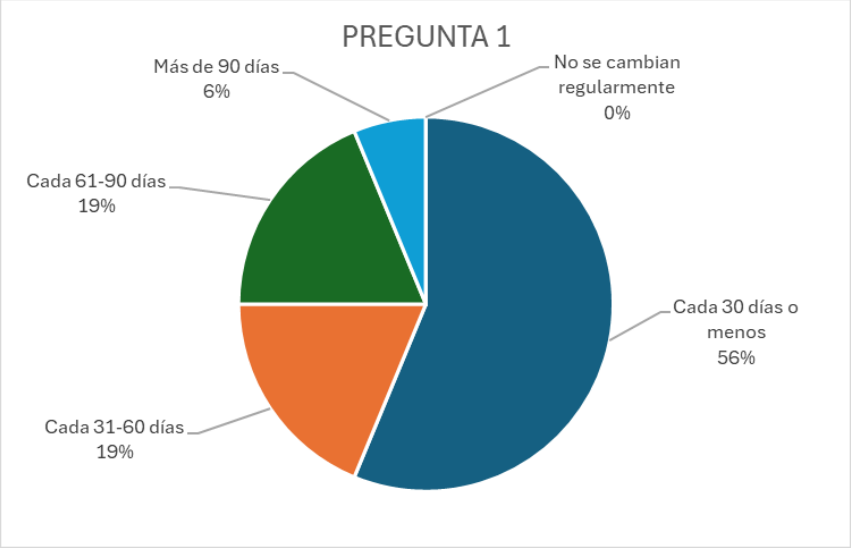
Tabla 5 ¿Con qué frecuencia cambia las contraseñas de acceso a los sistemas críticos?

VARIABLE	FRECUENCIA	PORCENTAJE
Cada 30 días o menos	9	56%

Cada 31-60 días	3	19%
Cada 61-90 días	3	19%
Más de 90 días	1	6%
No se cambian regularmente	0	0,00%
TOTAL	**16**	**100,00%**

Fuente: Personal de AIRMAXTELECOM S.A

La mayoría de los usuarios 56% sigue prácticas recomendadas al cambiar sus contraseñas cada 30 días o menos, lo que es un indicador favorable para la seguridad general de los servidores Mikrotik. Sin embargo, el 44% restante tiene la práctica de cambio menos frecuentes (más de 30 días), con un pequeño grupo 6% que extiende este período a más de 90 días. Esto representa un área de vulnerabilidad que podría ser aprovechada en ataques dirigidos, especialmente si las contraseñas no son complejas o están expuestas a riesgos como el phishing.



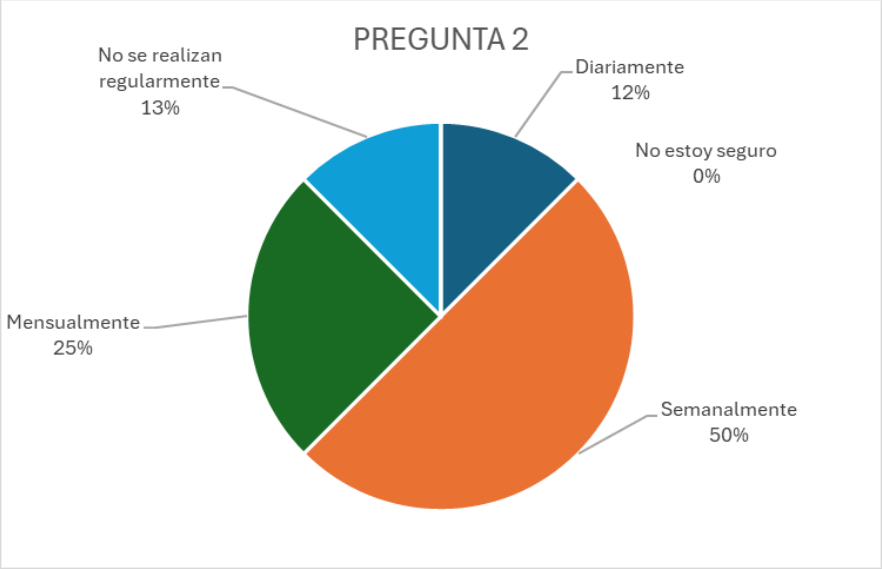
Fuente: Personal de AIRMAXTELECOM S.A

Tabla 6 ¿Con qué frecuencia se realizan respaldos de la información crítica en los servidores de borde?

VARIABLE	FRECUENCIA	PORCENTAJE
Diariamente	2	13%
Semanalmente	8	50%
Mensualmente	4	25%
No se realizan regularmente	2	13%
No estoy seguro	0	0%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

El 50% que realiza respaldos semanalmente puede estar adoptando un enfoque práctico, dependiendo del volumen y criticidad de los datos, pero existe un 38% que maneja respaldos con menos frecuencia (mensual o irregularmente), lo que deja abierta la posibilidad de pérdida significativa de información en caso de una emergencia. El 13% que no realiza respaldos regularmente está en una posición vulnerable ante posibles ataques, fallos del sistema o errores humanos, lo que podría afectar gravemente la continuidad del negocio.



Fuente: Personal de AIRMAXTELECOM S.A

Tabla 7 ¿Qué nivel de conocimiento tiene sobre los tipos de ataques cibernéticos a los que están expuestos los servidores de borde?

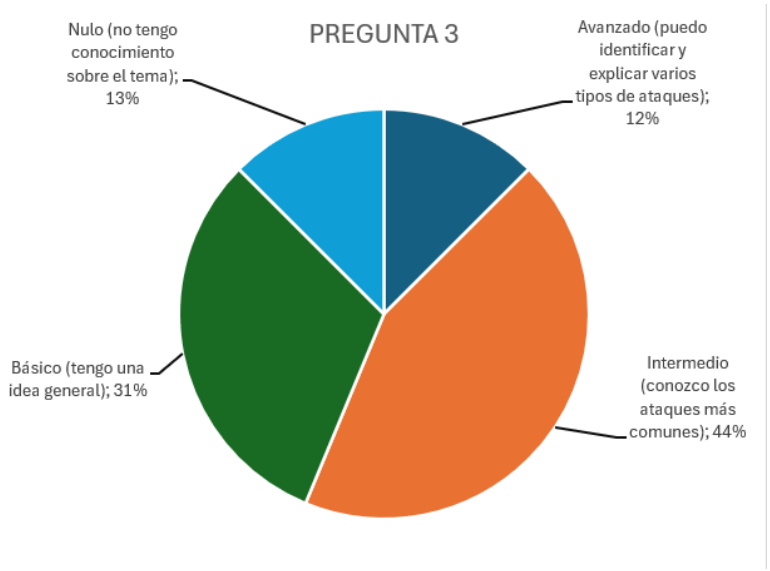
VARIABLE	FRECUENCIA	PORCENTAJE
Avanzado (puedo identificar y explicar varios tipos de ataques)	2	13%
Intermedio (conozco los ataques más comunes)	7	44%
Básico (tengo una idea general)	5	31%
Nulo (no tengo conocimiento sobre el tema)	2	13%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

El 44% de los encuestados tiene un conocimiento intermedio sobre los tipos de ataques cibernéticos, lo cual es alentador, solo una pequeña fracción 13% posee un nivel avanzado de comprensión de ataques. Esto significa que, si bien la mayoría tiene una idea de los

riesgos cibernéticos, solo un grupo reducido tiene las habilidades necesarias para actuar de manera proactiva ante estos ataques.

El 31% con conocimientos básicos y el 13% con conocimientos nulos son áreas de oportunidad que necesitan ser reforzadas. La falta de capacitación adecuada en estos grupos podría aumentar la vulnerabilidad de la organización frente a ciberataques, especialmente en la aplicación de las seguridades para los servidores de borde, que son puntos críticos en la infraestructura.



Fuente: Personal de AIRMAXTELECOM S.A

Tabla 8 ¿Cuándo fue su última capacitación formal sobre ciberseguridad y protección de sistemas?

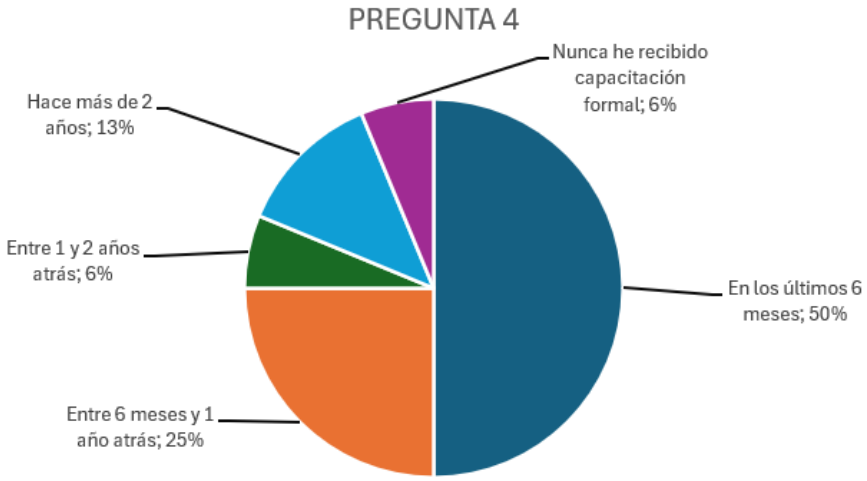
VARIABLE	FRECUENCIA	PORCENTAJE
En los últimos 6 meses	8	50%
Entre 6 meses y 1 año atrás	4	25%
Entre 1 y 2 años atrás	1	6%
Hace más de 2 años	2	13%
Nunca he recibido capacitación formal	1	6%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

En la empresa AIRMAXTELECOM S.A., el 50% del personal ha recibido capacitación en los últimos 6 meses muestra un buen nivel de actualización, lo cual es vital para mantener una postura de seguridad actualizada. Sin embargo, el hecho de que un 25% haya recibido capacitación hace más de un año, y que otro 19% (más de 2 años o nunca) no esté

actualizado, plantea preocupaciones sobre la falta de preparación en una parte significativa del equipo.

La ausencia de una capacitación reciente en ciertos empleados que administran los servidores y personal de las sucursales que también tienen accesos a los servidores Mikrotik implica que los conocimientos y habilidades de protección contra amenazas modernas pueden estar obsoletos, lo que incrementa la vulnerabilidad de la infraestructura tecnológica de la organización.



Fuente: Personal de AIRMAXTELECOM S.A

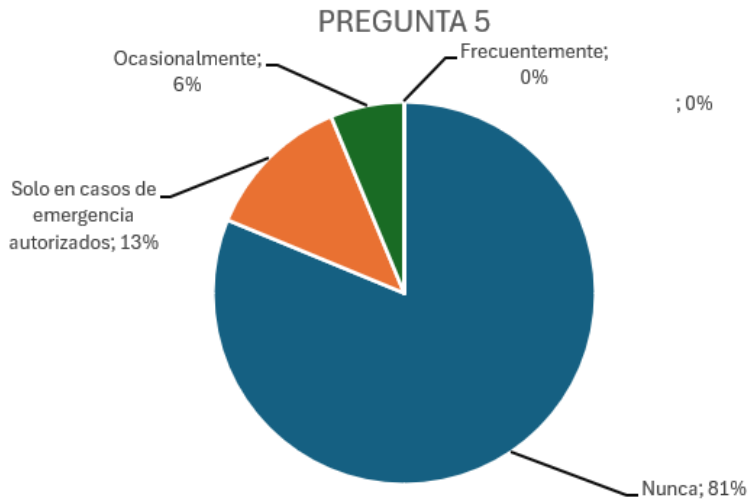
Tabla 9 ¿Comparte las credenciales de acceso (usuario y contraseña) con otros compañeros de trabajo?

VARIABLE	FRECUENCIA	PORCENTAJE
Nunca	13	81%
Solo en casos de emergencia autorizados	2	13%
Ocasionalmente	1	6%
Frecuentemente	0	0%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

El 81% de los empleados, es decir la gran parte de la empresa está comprometido y siguen buenas prácticas de seguridad al no compartir sus credenciales, lo que indica un nivel aceptable de concienciación sobre la importancia de la seguridad de la información. Sin embargo, el 6% que comparte ocasionalmente las credenciales es una preocupación, ya que el acceso compartido puede abrir la puerta a incidentes de seguridad, especialmente si no se lleva un control estricto.

El restante 13% que comparten credenciales solo en casos de emergencia deben asegurarse de que estos eventos estén bien documentados y se utilicen controles adicionales, como la autenticación multifactor, para limitar los riesgos.



Fuente: Personal de AIRMAXTELECOM S.A

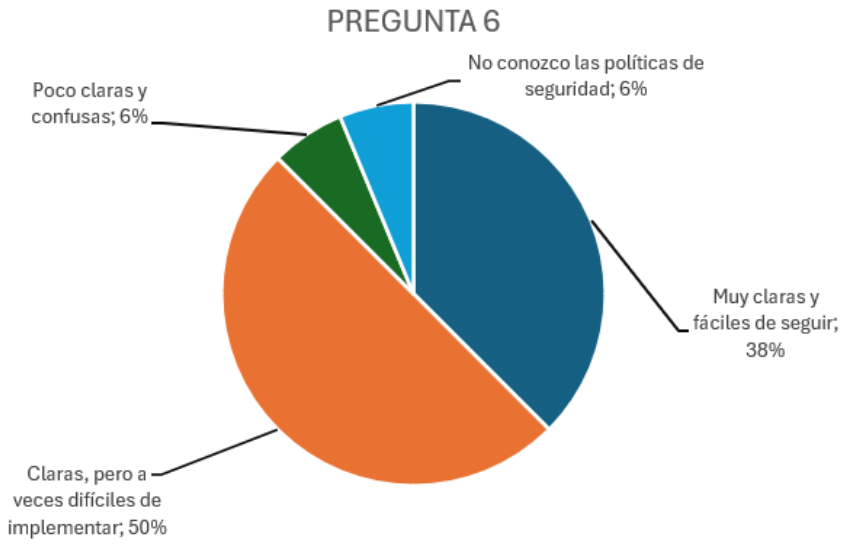
Tabla 10 ¿Qué tan claras y fáciles de seguir considera las políticas de seguridad de la información de la empresa?

VARIABLE	FRECUENCIA	PORCENTAJE
Muy claras y fáciles de seguir	6	38%
Claras, pero a veces difíciles de implementar	8	50%
Poco claras y confusas	1	6%
No conozco las políticas de seguridad	1	6%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

Es positivo que la mayoría de los encuestados considere que las políticas son claras, ya que esto muestra que existe un nivel adecuado de comunicación. Sin embargo, el 50% que encuentra dificultades en la implementación es un área que requiere atención. Las políticas, aunque claras, deben ser prácticas y aplicables en el día a día sin sobrecargar al personal.

Los grupos que consideran las políticas confusas o que no las conocen representan un riesgo, ya que su falta de claridad o desconocimiento puede generar vulnerabilidades en la seguridad de la información. Si estas personas no están alineadas con las normativas, es probable que puedan cometer errores que comprometan la seguridad.



Fuente: Personal de AIRMAXTELECOM S.A

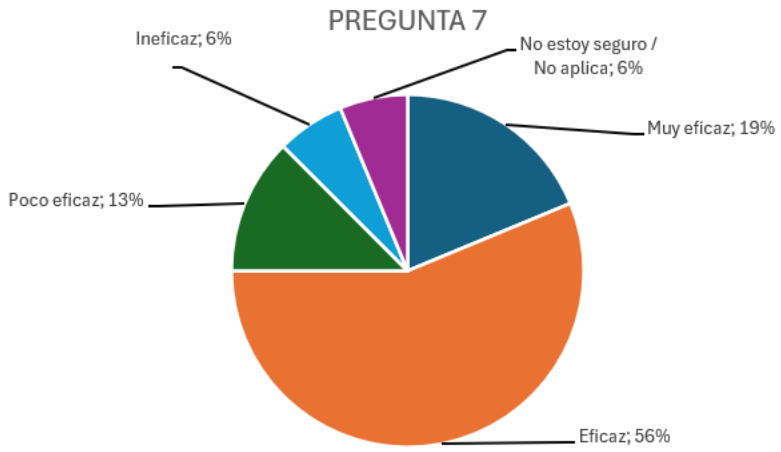
Tabla 11 ¿Cómo calificaría la eficacia del sistema de protección contra ataques de denegación de servicio (DDoS)?

VARIABLE	FRECUENCIA	PORCENTAJE
Muy eficaz	3	19%
Eficaz	9	56%
Poco eficaz	2	13%
Ineficaz	1	6%
No estoy seguro / No aplica	1	6%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

La mayoría de los empleados el 75% tiene una percepción positiva de la protección contra DDoS, con un 19% calificando el sistema como muy eficaz y un 56% como eficaz. Esto sugiere que, en términos generales, las medidas de defensa implementadas están funcionando bien para mitigar este tipo de ataques, proporcionando un nivel adecuado de protección.

Sin embargo, el 13% que considera el sistema como poco eficaz y el 6% que lo evalúa como ineficaz revelan áreas donde podrían existir vulnerabilidades o donde las expectativas no se están cumpliendo adecuadamente. Además, la falta de certeza por parte de otro 6% refleja la necesidad de mayor concienciación o transparencia sobre el funcionamiento del sistema de protección.



Fuente: Personal de AIRMAXTELECOM S.A

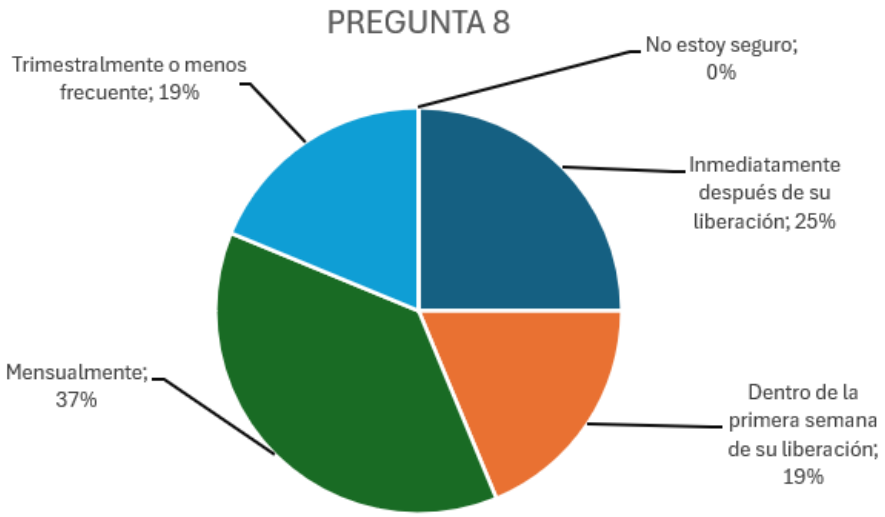
Tabla 12 ¿Con qué frecuencia se aplican actualizaciones de seguridad en los sistemas críticos?

VARIABLE	FRECUENCIA	PORCENTAJE
Inmediatamente después de su liberación	4	25%
Dentro de la primera semana de su liberación	3	19%
Mensualmente	6	38%
Trimestralmente o menos frecuente	3	19%
No estoy seguro	0	0%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

El 25% de los encuestados aplican actualizaciones inmediatamente y el 19% en la primera semana después de su liberación, lo que es positivo desde el punto de vista de la seguridad, ya que este grupo de usuarios se asegura de que las vulnerabilidades conocidas sean mitigadas lo más rápido posible.

Sin embargo, 38% de los participantes reporta que las actualizaciones se implementan mensualmente, y un 19% indica que se aplican trimestralmente o con menor frecuencia. Esto es preocupante, ya que las actualizaciones críticas que corrigen vulnerabilidades deben aplicarse lo antes posible para reducir el riesgo de explotación. Actualizar con menor frecuencia puede dejar los sistemas expuestos durante periodos prolongados, lo que puede ser aprovechado por atacantes.



Fuente: Personal de AIRMAXTELECOM S.A

Tabla 13 ¿Ha sido testigo o ha tenido conocimiento de intentos de ataque o brechas de seguridad en los servidores de borde en los últimos 12 meses?

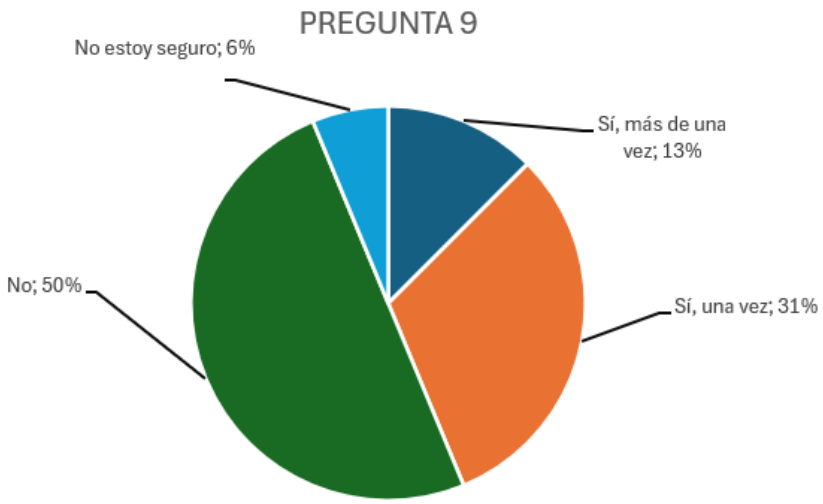
VARIABLE	FRECUENCIA	PORCENTAJE
Sí, más de una vez	2	13%
Sí, una vez	5	31%
No	8	50%
No estoy seguro	1	6%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

Los datos revelan que la mitad de los encuestados 50% no tiene conocimiento de intentos de ataque o brechas de seguridad en los servidores de borde en los últimos 12 meses, lo que podría sugerir que las medidas de seguridad implementadas son relativamente eficaces, o que la detección y comunicación de estos incidentes no es completamente clara o accesible para todos los empleados.

Por otro lado, el 44% de los participantes, es decir, 7 personas han tenido conocimiento de al menos un intento de ataque o brecha de seguridad, con un 13% habiendo sido testigos de múltiples intentos. Esto pone de manifiesto que, aunque la seguridad puede estar funcionando en muchos casos, existe un riesgo persistente de ataques que debería ser monitoreado de manera continua.

El 6% de los encuestados que no está seguro podría indicar una falta de visibilidad o comunicación sobre incidentes de seguridad, lo que sugiere la necesidad de mejorar la transparencia y el flujo de información en torno a estos eventos.



Fuente: Personal de AIRMAXTELECOM S.A

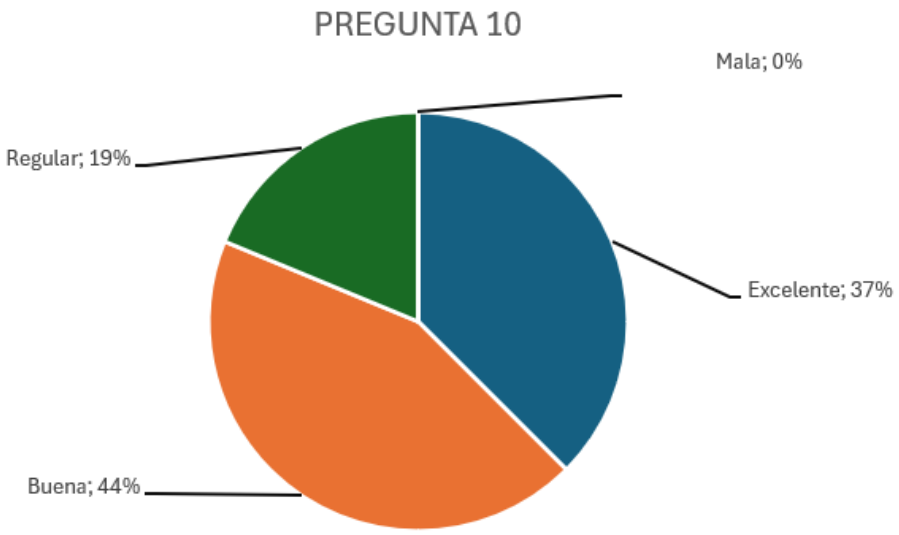
Tabla 14 ¿Cómo calificaría la gestión general de la seguridad de la información en la empresa?

VARIABLE	FRECUENCIA	PORCENTAJE
Excelente	6	38%
Buena	7	44%
Regular	3	19%
Mala	0	0%
TOTAL	**16**	**100%**

Fuente: Personal de AIRMAXTELECOM S.A

Los resultados indican que una mayoría combinada del 82%, es decir 13 personas considera que la gestión de la seguridad de la información es al menos buena o excelente, lo cual es un indicio positivo del desempeño general en esta área dentro de la empresa. El hecho de que ningún participante la califique como mala también sugiere que no hay percepciones de graves problemas en la gestión de la seguridad.

Sin embargo, un 19% que la valora como regular muestra que hay inquietudes en torno a ciertos aspectos de la seguridad que podrían no estar cumpliendo con las expectativas o estándares necesarios. Estos puntos de vista resaltan áreas donde la empresa puede optimizar o revisar sus prácticas.



Fuente: Personal de AIRMAXTELECOM S.A

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Aunque la mayoría de los empleados cambian sus contraseñas regularmente, existe un pequeño grupo que no lo hace con la frecuencia recomendada, lo cual representa un riesgo para la seguridad de los sistemas críticos. Asimismo, el uso de contraseñas simples sigue siendo un problema en algunas áreas. Por otra parte, si bien los respaldos de información son críticos y se realizan con cierta regularidad, no todos los usuarios hacen copias diarias, lo que puede suponer un riesgo en caso de pérdida de datos importantes.

En cuanto a la capacitación, un número significativo de empleados ha recibido formación en ciberseguridad. No obstante, hay un pequeño grupo que sigue sin estar entrenado formalmente, lo que representa un punto vulnerable dentro de la organización. En este sentido, aunque la mayoría de los empleados considera que las políticas son claras, algunos encuentran dificultades para implementarlas o las consideran confusas. Esto sugiere que, si bien las políticas existen, su aplicabilidad podría mejorarse.

La mayoría de los empleados considera eficaz el sistema de protección contra ataques de denegación de servicio, pero algunos tienen dudas sobre su efectividad o no están lo suficientemente informados al respecto. Por otro lado, la auditoría de los servidores Mikrotik reveló algunas vulnerabilidades (como problemas en SSL/TLS) y la presencia de puertos

abiertos en servidores clave, lo que sugiere que es necesario seguir con la actualización y monitoreo regular de los sistemas.

Los resultados de las pruebas de phishing revelaron que algunos administradores proporcionaron credenciales sin confirmar la autenticidad de los correos electrónicos, lo que muestra una debilidad en la capacitación sobre ingeniería social y la necesidad de concienciación continua.

RECOMENDACIONES

Es necesario implementar una política más estricta que requiera la actualización de contraseñas cada 60 días o menos. También se debe promover el uso de contraseñas más complejas, que sean difíciles de descifrar, y la implementación de la autenticación multifactor (MFA) en todos los sistemas críticos.

Se recomienda establecer un procedimiento que asegure respaldos diarios de la información más importante, de ser posible automatizar el proceso y estar verificando regularmente la integridad de estos. El personal debe ser educado sobre la importancia de los respaldos para garantizar una seguridad proactiva.

Es muy importante que todos los empleados, especialmente aquellos que no han recibido capacitación reciente o formal, participen en programas obligatorios de formación. Estas capacitaciones deben incluir simulaciones de phishing y ejercicios prácticos de respuesta a incidentes, para que los empleados estén preparados ante posibles ataques.

Se deben revisar las políticas ya que algunos empleados encuentran difíciles de implementar, adaptándolas a sus necesidades sin comprometer la seguridad de la empresa. También es importante reforzar la comunicación interna, asegurándose de que las políticas estén al alcance de todos y se comprendan claramente.

Reducir los tiempos de exposición de las vulnerabilidades, asegurando que las actualizaciones de seguridad críticas se apliquen dentro de la primera semana de su liberación. La automatización de este proceso puede ser una solución eficiente que reduzca los errores humanos y agilice las actualizaciones.

Dado el éxito parcial de las pruebas de phishing, es fundamental reforzar la capacitación en temas de ingeniería social. Simulaciones regulares de intentos de phishing ayudarán a evaluar y mejorar la respuesta de los empleados frente a estas amenazas.

REFERENCIAS Y BIBLIOGRAFIA

[SEMPLADES], S. N. (2027). Plna Nacional de Desarrollo.

Acosta, M. G. (2020). *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios.*

Administracion-Electronica. (octubre de 2014). *Administracion-Electronica*. Obtenido de MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Agudelo, D. A. (2022). Plan de Seguridad Informática. En P. d. Informática, *Plan de Seguridad Informática.* Medellin.

Aguilera, P. (2010). *Seguridad Informática.* Madrid: Editex.

ALULEMA, L. I. (2018). *ESTUDIO DE AMENAZAS Y VULNERABILIDADES EN LA INFRAESTRUCTURA TECNOLÓGICA DEL CENTRO TECNOLÓGICO DISGRAPTEC DE LA CIUDAD DE MONTALVO.* BABAHOYO: UNIVERSIDAD TECNICA DE BABAHOYO.

Ana Abril, J. P. (2013). ANÁLISIS DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN. *Universitaria Juan de Castellanos*.

Andersson, K. (2017). Autenticación más sólida para contraseña Credencial Servicios de Internet. *Booth, T., & Andersson, K. (2017). Stronger authentication for password credential Internet Services. 2017 Third International Conference on Mobile and Secure Services (MobiSecServ). doi:10.1109/mobisecserv.2017.7886566* .

Asamblea-Nacional-Del-Ecuador. (2021). *LEY ORGÁNICA DE PROTECCIÓN.* Quito.

Bar, J. R. (2018). Machine Learning, A Tutorial with R. *IEEE*, 8.

Buendía, J. F. (2013). *Seguridad informática.* McGraw-Hill.

Cerón, J. M., Scholten, C., Pras, A., & Santana, J. (2020). Panorama de dispositivos MikroTik, Honeypots realistas y clasificación de ataques automatizada. *IEEE EXPLORE*.

Cybersecurity), E. (. (s.f.). *enisa*. Obtenido de https://www.enisa.europa.eu/

Digital, B. (mayo de 2017). *Metodología de Pruebas de Intrusión en la NIST SP 800-115*. Obtenido de https://henryraul.wordpress.com/2017/05/10/metodologia-de-pruebas-de-intrusion-en-la-nist-sp-800-115/

Ecucert. (2017). *Ecucert*. Obtenido de EcuCERT de Arcotel – Centro de Respuesta a Incidentes Informáticos de la ARCOTEL. : https://www.ecucert.gob.ec/

GlobalSuit. (22 de septiembre de 2023). *GlobalSuit*. Obtenido de ¿Qué es la norma ISO 27001 y para qué sirve?: https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27001-y-para-que-sirve/

Hernández, R. O. (2003). Elementos teórico-prácticos útiles para conocer los virus informáticos. *ACIMED*.

Internet, L. U. (11 de Diciembre de 2019). *La Universidad en Internet*. Obtenido de La Universidad en Internet. Obtenido de ¿Qué es la certificación ISO 27001 y para qué sirve?: https://n9.cl/ibx3j

Jiménez, J. N. (2021). *MAPEO SISTEMÁTICO DE METODOLOGÍAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONTROL DE INFORMACIÓN PARA EL CONTROL DE LA GESTIÓN DE RIESGOS INFORMÁTICOS .* Guayaquil: UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL.

Leidy Johanna Cárdenas Solano, H. M. (2016). GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: REVISIÓN BIBLIOGRÁFICA.

Lopez, P. A. (2010). *Seguridad Informática.* Madrid: EDITEX.

MARK, M. (2014). *Theft of Service-Inevitable? Network.*

Orellana, R. J. (2021). *Diseño de la estructura de un manual de políticas de seguridad de la información para la Unidad de Informática del Gobierno Autónomo Descentralizado Municipal del Cantón Camilo Ponce Enríque.* Cuenca.

Parias, J. Q. (2016). *DISEÑO E IMPLEMENTACIÓN DE RED GESTION OTM.*

Quispe, C. A. (2010). TIPOS DE HACKERS. *Universidad Mayor de San Andrés*.

Richet, J.-L. (2013). *From Young Hackers to Crackers.*

Shaikh, A. P. (7 de abril de 2020). *SSRN*. Obtenido de SSRN: https://doi.org/10.2139/SSRN.3568728

Villafuerte, J. R. (2014). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA CENTRAL PRIVADA DE INFORMACIÓN DE RIESGOS. En J. R. Villafuerte, *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA UNA CENTRAL PRIVADA DE INFORMACIÓN DE RIESGOS.* Lima.

wallarm. (23 de febrero de 2023). *wallarm*. Obtenido de ¿Qué Es El Análisis Factorial De Riesgo De La Información (FAIR)?: https://www.wallarm.com/what/what-is-factor-analysis-of-information-risk-fair

ANEXOS

ANEXO A: POLITICADE LA SEGURIDAD DE LA INFORMACION AIRMAXTELECOM S.A

https://drive.google.com/file/d/1lEOGEK7Qv6YWc69i5Uv41d4nDy-FEM_S/view?usp=drive_link

ANEXO B: METODOLOGIA NIST SP 800-115

https://drive.google.com/file/d/19FtSBHJ-upSOn1oIS7uRQIbHdHzyVWmR/view?usp=drive_link

ANEXO C: CARTA DE CONFICENCIALIDAD AIRMAXTELECOM S.A

https://drive.google.com/file/d/1KHH0a-I2XofzZFirG_MyCbVmPfBCLiLn/view?usp=drive_link

ANEXO D: CIRCULAR DE RESPONSABILIDAD DE USO DE SISTEMA

https://drive.google.com/file/d/1HQ_Pega8wwTEEHRZzLhoJsEkurssaMIR/view?usp=drive_link