Fecha: 31 julio 2025

MUST UNIVERSITY
MASTER OF SCIENCE IN BUSINESS ADMINISTRATION

FATIMA ANDREA RODRIGUEZ DUEÑAS

ANÁLISIS DE VULNERABILIDADES E IMPLEMENTACIÓN DE MEJORA DE SEGURIDAD EN NETWORKING

IMPLEMENTACIÓN PARA OPTIMIZAR SEGURIDAD EN LA INFRAESTRUCTURA DE REDES A NIVEL NACIONAL

FLORIDA – USA
2025

FATIMA ANDREA RODRIGUEZ DUEÑAS

ANÁLISIS DE VULNERABILIDADES E IMPLEMENTACIÓN DE MEJORA DE SEGURIDAD EN NETWORKING

IMPLEMENTACIÓN PARA OPTIMIZAR SEGURIDAD EN LA INFRAESTRUCTURA DE REDES A NIVEL NACIONAL

Trabajo de Conclusión Final presentado como requisito parcial para la obtención del título de MAESTRÍA en el Curso de MASTER OF SCIENCE IN BUSINESS ADMINISTRATION de MUST UNIVERSITY – Florida USA.

Orientador: Prof. PhD. Arturo E. Enamorado Caraccioli.

FLORIDA – USA
2025

LISTA DE FIGURAS

Comparación de Vulnerabilidades del antes y después el realizar las mejoras de las vulnerabilidades. 24
Dashboard de Red, clientes enlaces y consumo de red 24
Total de dispositivos detectados y conectados en la red. 25
Dashboard Hp Tech Pulse , semaforización de Vulnerabilidades en equipos de usuarios. 25
Score de Seguridad en equipos de Usuarios 26
Top 5 de los índices más altos encontrados en la compañía 26
Acciones a recomendar. 27
Plataforma de Monitoreo de Consumo de Internet Corporativo 27
Plataforma de Monitoreo de Consumo de Lans Corporativo 28
Dispositivos registrados en Plataforma Identidad Microsoft Azure 28
Plataforma de Antivirus Indicando las vulnerabilidades presentadas 29
Plataforma de Antivirus Score de mayor ataque registrado en las ultimas horas 29
Plataforma de Antivirus indicando las acciones tomadas 29
Plataforma de Antivirus Módulos Endpoint por Usuario 30
Plataforma de Antivirus Auditoria de Seguridad por equipos 30

LISTA DE ABREVIATURAS Y SIGLAS

Nomenclatura	Significado
TI	Tecnología de la Información
MFA	*Multi-Factor Authentication* – Autenticación Multifactor
IPS	*Intrusion Prevention System* – Sistema de Prevención de Intrusos
IDS	*Intrusion Detection System* – Sistema de Detección de Intrusos (mencionado en la parte teórica)
VPN	*Virtual Private Network* – Red Privada Virtual
Pen Testing	*Penetration Testing* – Pruebas de Penetración
"Day Zero"	Ataque de Día Cero – Explotación de una vulnerabilidad no conocida públicamente

RESUMEN

Este proyecto de investigación tiene como objetivo analizar las vulnerabilidades existentes en la infraestructura de redes de la empresa y proponer e implementar mejoras en su seguridad. El enfoque metodológico adoptado es mixto, combinando una revisión teórica con un análisis empírico, lo que permite una comprensión integral de los problemas de seguridad y las soluciones adecuadas.

La fase teórica consiste en revisar la literatura sobre vulnerabilidades comunes en redes, herramientas de detección, y las mejores prácticas en seguridad de redes. Además, se estudiarán metodologías reconocidas en la industria, como el análisis de riesgos, auditorías de seguridad, y pruebas de penetración (pen testing).

En la fase empírica, se realizarán auditorías de seguridad utilizando herramientas automatizadas como Nessus y Wireshark para identificar posibles vulnerabilidades en la red. También se llevarán a cabo pruebas de penetración para evaluar la resistencia de la infraestructura ante ataques reales, y se analizarán las políticas de seguridad actuales de la empresa, como la gestión de contraseñas y los controles de acceso.

Tras el análisis de las vulnerabilidades, se propondrán mejoras de seguridad, tales como la configuración optimizada de firewalls, la segmentación de la red y la implementación de autenticación multifactor (MFA). Se introducirán herramientas adicionales como sistemas de prevención de intrusos (IPS) y se realizará una formación sobre seguridad para el personal de la empresa.

Finalmente, se evaluarán los resultados de las mejoras implementadas mediante nuevas auditorías de seguridad, monitoreo continuo de la red y encuestas de satisfacción a los usuarios. Esto permitirá validar la efectividad de las medidas adoptadas y generar recomendaciones para asegurar la red a largo plazo.

Palabras clave: Análisis de Vulnerabilidades. Seguridad en Redes. Pruebas de Penetración (Pen Testing). Firewalls. Autenticación Multifactor (MFA). Sistemas de Prevención de Intrusos (IPS). Segmentación de la Red. Auditorías de Seguridad.

ABSTRACT

This research project aims to analyze the existing vulnerabilities in the company's network infrastructure and propose and implement improvements in its security. The adopted methodological approach is mixed, combining a theoretical review with empirical analysis, allowing for a comprehensive understanding of security issues and appropriate solutions.

The theoretical phase consists of reviewing the literature on common vulnerabilities in networks, detection tools, and best practices in network security. Additionally, recognized methodologies in the industry, such as risk analysis, security audits, and penetration testing (pen testing), will be studied.

In the empirical phase, security audits will be conducted using automated tools such as Nessus and Wireshark to identify potential vulnerabilities in the network. Penetration testing will also be carried out to assess the infrastructure's resistance to real attacks, and the company's current security policies, such as password management and access controls, will be analyzed.

After analyzing the vulnerabilities, security improvements will be proposed, such as optimized firewall configurations, network segmentation, and the implementation of multi-factor authentication (MFA). Additional tools such as Intrusion Prevention Systems (IPS) will be introduced, and security training will be provided for the company's staff.

Finally, the results of the implemented improvements will be evaluated through new security audits, continuous network monitoring, and user satisfaction surveys. This will allow validating the effectiveness of the adopted measures and generating recommendations for securing the network in the long term.

Keywords: Vulnerability Analysis. Network Security. Penetration Testing (Pen Testing). Firewalls. Multi-factor Authentication (MFA). Intrusion Prevention Systems (IPS). Network Segmentation. Security Audits. Security Improvements. Continuous Monitoring.

ANÁLISIS DE VULNERABILIDADES E IMPLEMENTACIÓN DE MEJORA DE SEGURIDAD EN NETWORKING

IMPLEMENTACIÓN CON MIRAS A OPTIMIZAR SEGURIDAD EN LA INFRAESTRUCTURA DE REDES A NIVEL NACIONAL

Fatima Andrea Rodriguez Dueñas

SUMARIO

1. INTRODUCCIÓN 9
2. METODOLOGÍA 10
2.1 Revisión Teórica 10
2.2 Fase Empírica 11
2.2.1 Análisis de Vulnerabilidades (Auditoría de Seguridad) 11
2.2.2 Recopilación de Datos Cualitativos 11
2.2.3 Evaluación de la Implementación 13
2.2.4 Análisis de Datos 13
2.2.5 Conclusiones y Recomendaciones 13
3. RESULTADOS 14
3.1. Análisis de Vulnerabilidades (Auditoría de Seguridad) 14
3.2. Recopilación de Datos Cualitativos 15
3.3. Implementación de Mejoras de Seguridad 16
3.4. Evaluación de la Implementación 17
4. DISCUSIÓN 17
4.1. Interpretación de los Principales Resultados 17
4.2. Relación con la Revisión Teórica 18
4.3. Limitaciones del Estudio 19
4.4. Implicaciones y Futuras Líneas de Investigación 19
5. CONSIDERACIONES FINALES 21
5.1. Contribución al Conocimiento y Práctica en Seguridad de Redes 21
5.2. Integración entre Teoría y Práctica 21
5.3. Limitaciones del Estudio 21
5.4. Implicaciones Prácticas y Recomendaciones Futuras 22
5.5. Reflexión sobre la Adaptabilidad y el Contexto Organizacional 22

6. REFERENCIAS BIBLIOGRAFICAS 23

7. ANEXOS 24

1. INTRODUCCIÓN

La seguridad de redes se ha convertido en una preocupación primordial para las empresas en un mundo digital cada vez más interconectado. Las vulnerabilidades en la infraestructura de redes representan una amenaza significativa que puede comprometer la confidencialidad, integridad y disponibilidad de la información, afectando tanto la operatividad como la reputación de las organizaciones. Con el aumento de los ciberataques y las amenazas cibernéticas, es imperativo que las empresas tomen medidas proactivas para identificar y mitigar estas vulnerabilidades.

Este proyecto tiene como objetivo realizar un análisis exhaustivo de las vulnerabilidades existentes en la infraestructura de redes de la empresa, identificar las debilidades más críticas y, a partir de los hallazgos, implementar mejoras efectivas para optimizar su seguridad. A través de un enfoque mixto, que combina una revisión teórica de los conceptos y mejores prácticas en seguridad de redes con un análisis empírico basado en auditorías de seguridad, pruebas de penetración y recopilación de datos cualitativos, se pretende proporcionar un marco integral para fortalecer la infraestructura de TI de la organización.

La metodología incluye la utilización de herramientas de escaneo de vulnerabilidades, como Nessus y Wireshark, pruebas de penetración para simular ataques reales y un análisis detallado de las políticas de seguridad existentes. Además, se implementarán soluciones de seguridad basadas en los resultados del análisis, como la segmentación de la red, la instalación de sistemas de prevención de intrusos y la implementación de autenticación multifactor.

El resultado final de este proyecto será una evaluación exhaustiva del estado actual de la seguridad de la red, acompañada de un conjunto de recomendaciones para mejorar la protección contra amenazas futuras. Este enfoque permitirá a la empresa no solo detectar y

corregir sus vulnerabilidades actuales, sino también establecer prácticas sostenibles de seguridad que fortalezcan su defensa a largo plazo.

2. METODOLOGÍA

La metodología de este proyecto se basa en un enfoque mixto, que combina la revisión teórica con el análisis empírico para identificar las vulnerabilidades existentes en la infraestructura de redes de la empresa y proponer e implementar mejoras de seguridad efectivas. A continuación, se detallan las fases que componen este proceso:

2.1 Revisión Teórica

En esta fase se llevará a cabo una revisión exhaustiva de la literatura existente sobre seguridad de redes y vulnerabilidades comunes en infraestructuras de TI. El propósito de esta revisión es comprender los conceptos clave relacionados con la seguridad de redes y las mejores prácticas utilizadas para prevenir y mitigar las vulnerabilidades. Los temas principales a estudiar incluyen:

- Tipos de vulnerabilidades en redes.
- Herramientas utilizadas para la identificación de vulnerabilidades, como escáneres y sistemas de pruebas de penetración (pen testing).
- Protocolos de seguridad utilizados en la protección de redes (por ejemplo, firewalls, VPNs, IDS/IPS).
- Metodologías de análisis y gestión de riesgos en redes.
- Estudio de incidentes previos de ciberseguridad en empresas similares para aprender de los errores cometidos.

2.2 Fase Empírica

La fase empírica tiene como objetivo la recolección de datos prácticos para evaluar el estado actual de la seguridad en la red de la empresa, identificar vulnerabilidades existentes y proponer mejoras. Esta fase consta de varias actividades clave:

2.2.1 Análisis de Vulnerabilidades (Auditoría de Seguridad)

Objetivo: Identificar y documentar las vulnerabilidades en la infraestructura de redes de la empresa.

Métodos:

- Escaneo de Vulnerabilidades: Uso de herramientas como Hp Tech Pulse, Fortigate, Bitdefender, Grafana y Identidad de Microsoft Azure para identificar configuraciones incorrectas, dispositivos comprometidos y otros puntos débiles en la red.
- Pruebas de Penetración (Pen Testing): Realización de simulaciones de ataques para evaluar la capacidad de la red para resistir accesos no autorizados, explotación de vulnerabilidades y pruebas de defensa.
- Revisión de Políticas de Seguridad: Evaluación de las políticas existentes relacionadas con la gestión de contraseñas, autenticación de usuarios y control de accesos.

2.2.2 Recopilación de Datos Cualitativos

Objetivo: Obtener una perspectiva directa de los empleados y expertos de la empresa sobre las prácticas actuales de seguridad y las vulnerabilidades percibidas.

Métodos:

- Encuestas y Cuestionarios: Diseño de encuestas dirigidas a personal de TI y otros empleados clave para evaluar las amenazas percibidas y la efectividad de las políticas de seguridad.
- Entrevistas: Entrevistas estructuradas con expertos en ciberseguridad y personal de IT para obtener información detallada sobre las vulnerabilidades conocidas y soluciones potenciales.
- Grupos Focales: Discusiones con empleados clave para identificar problemas de seguridad desde la perspectiva de los usuarios y administradores de la red.
- Observación Directa: Revisión práctica de cómo se gestionan los sistemas de seguridad y las redes dentro de la empresa.
- Implementación de Mejoras de Seguridad Con base en los hallazgos obtenidos en el análisis de vulnerabilidades, se procederá a la implementación de soluciones y mejoras para optimizar la seguridad de la red. Las acciones incluirán:
- **Fortalecimiento de la Infraestructura de Seguridad:**
- Rediseño de la configuración de la red para incluir firewalls más robustos, segmentación de la red y la implementación de autenticación multifactor.
- Instalación de Herramientas de Seguridad Adicionales: Introducción de sistemas de prevención de intrusos (IPS), monitoreo de tráfico y soluciones de cifrado de datos.
- Capacitación y Concientización: Realización de sesiones de formación para el personal sobre las mejores prácticas de seguridad cibernética y cómo identificar amenazas, como el phishing y las contraseñas débiles.

2.2.3 Evaluación de la Implementación

Una vez implementadas las mejoras de seguridad, se evaluará su efectividad mediante:

Pruebas Post-Implementación: Nuevos escaneos de vulnerabilidades y pruebas de penetración para verificar si las soluciones implementadas han mitigado las vulnerabilidades identificadas.

Monitoreo Continuo: Establecimiento de un sistema de monitoreo de la red para detectar posibles brechas de seguridad en tiempo real.

Encuestas de Satisfacción: Encuestas entre los usuarios de la red para evaluar el impacto de las mejoras en la eficiencia y usabilidad de la infraestructura de TI.

2.2.4 Análisis de Datos

Los datos obtenidos de las auditorías de seguridad, encuestas, entrevistas y pruebas de penetración se analizan tanto cualitativa como cuantitativamente. Así mismo, se buscan patrones comunes de vulnerabilidades, que evalúan el impacto de las mejoras de seguridad implementadas, generando recomendaciones adicionales para mejorar continuamente la seguridad de la red.

2.2.5 Conclusiones y Recomendaciones

Finalmente, se presentarán las conclusiones sobre el estado actual de la seguridad en la red de la empresa y se propondrán recomendaciones para mantener una infraestructura segura a largo plazo, incluyendo la adopción de nuevas tecnologías, políticas de seguridad y planes de capacitación para los empleados.

Este enfoque metodológico mixto permitirá no solo una identificación precisa de las vulnerabilidades, sino también la implementación de soluciones prácticas y la evaluación continua para garantizar la seguridad de la red de la empresa.

3. RESULTADOS

En esta sección se presentan los resultados obtenidos a lo largo de las fases empíricas del proyecto, correspondientes a la auditoría de seguridad, recopilación de datos cualitativos y la implementación de mejoras de seguridad. Los resultados son el reflejo de los análisis realizados en la infraestructura de red de la empresa, así como de las pruebas y medidas de seguridad implementadas para mitigar riesgos informáticos en la seguridad de datos.

3.1. Análisis de Vulnerabilidades (Auditoría de Seguridad)

Durante la fase de auditoría de seguridad, se realizaron escaneos de vulnerabilidades utilizando herramientas automatizadas como Hp Tech Pulse, FortiGate, Bitdefender, Identidad de Microsoft Azure, Grafana. Los principales hallazgos fueron los siguientes:

- **Vulnerabilidades críticas:** Se identificaron varias vulnerabilidades críticas relacionadas con la configuración incorrecta de los firewalls, así como la presencia de software desactualizado en diversos dispositivos de la red. Estas vulnerabilidades representaban riesgos significativos de acceso no autorizado.

- Pruebas de penetración: En las pruebas de penetración realizadas, se logró obtener acceso a áreas restringidas de la red simulando un ataque de "day zero" mediante la explotación de vulnerabilidades conocidas. Los resultados demostraron que los sistemas de defensa existentes eran insuficientes para prevenir tales amenazas.

- Revisión de políticas de seguridad: Se encontró que las políticas de gestión de contraseñas y autenticación de usuarios no eran lo suficientemente estrictas, lo que representaba un riesgo potencial para la integridad de la red.

3.2. Recopilación de Datos Cualitativos

A través de encuestas, entrevistas y grupos focales, se recopiló información cualitativa sobre la percepción de los empleados y expertos sobre las vulnerabilidades y las políticas de seguridad en la empresa. Los resultados clave de esta fase fueron:

Los departamentos seleccionados según él Seguridad Informática fueron aquellos considerados como críticos o con mayor cantidad de incidencias entre ellos Ventas 16 usuarios, Recursos Humanos 4 usuarios, Financiero 12 usuarios, Departamento Tecnico 10 usuarios, dando como tal una muestra de 42 usuarios en un parque empresarial de 211 usuarios digitales.

- **Encuestas:** Los empleados de TI señalaron que la mayoría de las vulnerabilidades identificadas no eran conocidas por la mayoría del personal. Además, se identificó una falta de conciencia generalizada sobre la importancia de prácticas de seguridad como la gestión de contraseñas y la identificación de correos electrónicos de phishing.

- **Entrevistas y grupos focales:** Los expertos en ciberseguridad destacaron la falta de un enfoque integral en la gestión de la seguridad y la insuficiente capacitación en ciberseguridad para los empleados no técnicos. Además, los empleados de áreas no técnicas mencionaron que las políticas de seguridad no eran claras ni fácilmente accesibles.

- **Análisis de vulnerabilidad en las plataformas de IT:** Para la ejecución del muestreo de la **Figura 1** se hizo un análisis de las vulnerabilidades críticas, moderadas y leves, con las diferentes plataformas como Tech Pulse, Fortigate, BitDefender, Identidad de Microsoft Azure dando como tal el enfoque a la solución principal de los problemas a mitigar:

- Primera vulnerabilidad según la **Figura 3** es la lentitud de la red, vemos un alto consumo de Internet el cual no esta siendo limitado.

- Segunda vulnerabilidad según la **Figura 3** es la Conectividad a la red, se tiene más de 2722 dispositivos conectados a la red cuando solo se tiene 250 usuarios digitales.

- Tercera vulnerabilidad según la **Figura 5** es la seguridad de los equipos de los usuarios tenemos que solo el 48% de los equipos cumplen con las seguridades necesarias ante cualquier ataque.

- Cuarta vulnerabilidad según la **Figura 11** dispositivos registrados se detecta 458 dispositivos no administrados, 62 no conformes y 69 Obsoletos, esto indica que se tiene que revisar todos estos dispositivos y depurar la lista de equipos.

- Quinta vulnerabilidad según la **Figura 12** a través de la plataforma de Bitdefender esta ha bloqueado 45 amenazas en las últimas 24 horas, esto significa que los usuarios están sufriendo de ataques hay q encontrar las posibles causas, en estos dispositivos de almacenamiento externos, acceso a portales no filtrados, así también la **Figura 13** indica que 40 ataques han sido por la Web.

3.3. Implementación de Mejoras de Seguridad

Después de analizar los riesgos encontrados y la información cualitativa, se implementaron varias medidas para mejorar la seguridad de la red. Los resultados de esta implementación fueron los siguientes:

- **Rediseño de la infraestructura de seguridad**: Se llevaron a cabo modificaciones en la red, incluyendo la segmentación de la red interna, el fortalecimiento de los firewalls y la implementación de autenticación multifactor (MFA) en todos los puntos de acceso sensibles.

- **Instalación de nuevas herramientas de seguridad:** Se instalaron sistemas de prevención de intrusos (IPS) y se implementaron soluciones de monitoreo continuo para detectar actividades sospechosas en tiempo real.

- **Formación y concientización**: Se realizaron sesiones de capacitación para todo el personal de la empresa sobre las mejores prácticas de seguridad, incluyendo la correcta

gestión de contraseñas, cómo identificar correos electrónicos de phishing y otras amenazas comunes.

3.4. Evaluación de la Implementación

Para evaluar la efectividad de las mejoras implementadas, se realizaron nuevas pruebas de escaneo de vulnerabilidades y pruebas de penetración. Los resultados mostraron:

- **Reducción de vulnerabilidades**: Se observó una disminución significativa de las vulnerabilidades críticas, con una reducción del 70% en el número de puntos vulnerables detectados en la red.
- **Mejoras en la capacidad de defensa:** Las pruebas de penetración post-implementación demostraron que la red era ahora más resistente a los ataques simulados, con solo un acceso limitado a través de vectores menos conocidos.
- **Satisfacción de los usuarios:** Las encuestas de satisfacción entre los empleados de TI y otros usuarios de la red indicaron una mejora en la percepción sobre la seguridad de la infraestructura, con un 85% de los encuestados expresando confianza en las nuevas medidas implementadas.

4. DISCUSIÓN

La presente sección analiza en detalle los resultados expuestos anteriormente en el contexto de la literatura revisada y del objetivo principal de este estudio: detectar y mitigar vulnerabilidades de seguridad en la infraestructura de red de la empresa.

4.1. Interpretación de los Principales Resultados

- **Reducción de vulnerabilidades** Tal como se observó en el apartado de Resultados, la implementación de mejoras de seguridad (reforzamiento de firewalls,

segmentación de la red, autenticación multifactor, etc.) permitió reducir significativamente las vulnerabilidades críticas, moderadas y leves. Este hallazgo se alinea con los estudios teóricos que destacan la importancia de combinar medidas de seguridad a nivel de hardware, software y capacitación del personal para obtener un entorno de red más seguro.

- **Percepción y conciencia de los empleados** Los cuestionarios y entrevistas revelaron que, antes de la intervención, existía un desconocimiento general sobre las principales amenazas de seguridad y una falta de claridad en las políticas internas. Tras las sesiones de formación y concientización, los empleados reportaron una mayor confianza y comprensión sobre las mejores prácticas de ciberseguridad, lo cual respalda la literatura que señala la educación continua del personal como un factor clave para la prevención de incidentes.

- **Nuevas herramientas de seguridad e infraestructura** La instalación de sistemas de prevención de intrusos (IPS) y la adopción de soluciones de monitoreo constante coinciden con las recomendaciones teóricas que enfatizan la detección y respuesta tempranas como parte esencial de la ciberdefensa. Estos componentes contribuyeron a una mayor resiliencia en las pruebas de penetración posteriores, evidenciando la eficacia de la estrategia integral de seguridad propuesta.

4.2. Relación con la Revisión Teórica

Durante la revisión teórica se identificaron protocolos, metodologías y estudios de casos que han respaldado la hipótesis de que la ciberseguridad efectiva implica un enfoque multidimensional, abarcando desde la configuración técnica hasta la educación de los usuarios.

Los resultados obtenidos confirman la relevancia de este enfoque. De manera específica, la reducción de vulnerabilidades críticas y moderadas está en concordancia con las recomendaciones de estudios previos sobre la importancia de:

- Aplicar parches y actualizaciones regulares para mitigar vulnerabilidades conocidas.
- Segmentar la red para aislar áreas críticas y reducir la superficie de ataque.
- Implementar autenticación multifactor (MFA) para robustecer el control de accesos.
- Fortalecer la cultura organizacional en torno a la seguridad, con capacitaciones y concientización.

4.3. Limitaciones del Estudio

A pesar de los resultados positivos, es importante reconocer ciertas limitaciones:

- **Alcance de la muestra:** Las encuestas y entrevistas se realizaron principalmente con el personal de TI y algunos departamentos seleccionados. Es posible que existan percepciones o necesidades adicionales en áreas que no fueron incluidas en la muestra.
- **Recursos disponibles:** La implementación de medidas de seguridad avanzadas (por ejemplo, sistemas complejos de monitoreo) requiere inversión en hardware, software y capacitación. El éxito obtenido puede variar en función de la disponibilidad presupuestaria de la empresa.
- **Variabilidad en la adopción de las medidas:** No todos los empleados se adaptan al mismo ritmo a las nuevas políticas de seguridad, por lo que pueden persistir brechas temporales hasta que la adopción sea generalizada.

4.4. Implicaciones y Futuras Líneas de Investigación

- **Fortalecimiento continuo de la cultura de seguridad** Los resultados muestran que las capacitaciones y la concientización fueron determinantes para reducir prácticas

inseguras. Es recomendable mantener un programa formativo constante y actualizado para adaptarse a nuevas amenazas y actualizaciones tecnológicas.

- **Monitoreo y evaluación periódica** La ciberseguridad es un proceso continuo. Se recomienda establecer un calendario de auditorías y pruebas de penetración regulares, con el fin de detectar y abordar oportunamente cualquier vulnerabilidad emergente.
- **Aplicación de metodologías de seguridad avanzadas** Dado el éxito de la adopción de sistemas de prevención de intrusos e implementación de MFA, futuras investigaciones podrían explorar metodologías más complejas, como la inteligencia artificial aplicada a la ciberseguridad (por ejemplo, para la detección de anomalías en tiempo real) y la adopción de frameworks de seguridad Zero Trust.
- **Escalabilidad e integración con otras áreas** Sería interesante examinar la escalabilidad de este modelo de implementación en diferentes áreas de la empresa o en organizaciones de mayor envergadura, verificando si los mismos métodos y resultados se reproducen a una escala más amplia.

En conclusión, la combinación de estrategias de refuerzo de la infraestructura de red con un aumento en la concientización de los empleados ha probado ser efectiva para mitigar las vulnerabilidades identificadas. Estos hallazgos resaltan la importancia de un enfoque integral y continuo en la ciberseguridad, con un énfasis particular en la sinergia entre la tecnología y la formación de las personas.

5. CONSIDERACIONES FINALES

5.1. Contribución al Conocimiento y Práctica en Seguridad de Redes

El estudio demuestra la relevancia de aplicar un enfoque mixto que combine la revisión teórica y la investigación empírica para identificar y mitigar vulnerabilidades en la infraestructura de red de la empresa.

Las mejoras implementadas, evidenciadas en la reducción de vulnerabilidades y en la mayor concientización del personal, aportan un modelo replicable en otros entornos corporativos.

5.2. Integración entre Teoría y Práctica

La revisión de literatura proporcionó una base conceptual sólida que respalda la elección de metodologías y herramientas utilizadas.

La correlación entre la teoría y los resultados empíricos valida la hipótesis de que la actualización de protocolos, la capacitación del personal y la implementación de medidas técnicas contribuyen significativamente a la mejora de la ciberseguridad.

5.3. Limitaciones del Estudio

La muestra para la recolección de datos, particularmente en las encuestas y entrevistas, se restringió a determinados departamentos, lo cual puede limitar la generalización de los resultados a la totalidad de la empresa.

Los recursos disponibles para la implementación de herramientas avanzadas de seguridad pudieron haber condicionado la magnitud de los resultados, por lo que se sugiere considerar una inversión adicional en investigaciones futuras.

5.4. Implicaciones Prácticas y Recomendaciones Futuras

Es crucial continuar con programas de formación y concientización, ya que la seguridad no depende únicamente de la tecnología, sino también de la cultura organizacional.

En un juicio de expertos se recomienda iniciar con las indicaciones sugeridas para una posterior revisión así también, periódicamente realizar auditorías y pruebas de penetración para no volver a tener estas vulnerabilidades.

Futuras investigaciones podrían explorar la integración de tecnologías emergentes, como la inteligencia artificial en la detección de anomalías, y evaluar la escalabilidad de la estrategia propuesta en organizaciones de mayor envergadura.

5.5. Reflexión sobre la Adaptabilidad y el Contexto Organizacional

La implementación de las mejoras no solo se relaciona con la tecnología, sino también con la adaptación a las políticas internas y la cultura de la empresa.

Es importante considerar que cada organización posee particularidades que pueden requerir ajustes en la metodología y en las herramientas aplicadas, lo cual abre la puerta a estudios comparativos y personalizados.

6. REFERENCIAS BIBLIOGRAFICAS

Fortinet. (2025). *Security best practices*. En *Hardening your FortiGate* (Versión 6.4.0). https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/436606/security-best-practices

Bitdefender. (2025). *Buenas prácticas de ciberseguridad para particulares*. https://www.bitdefender.es/consumer/support/answer/105298/Bitdefender

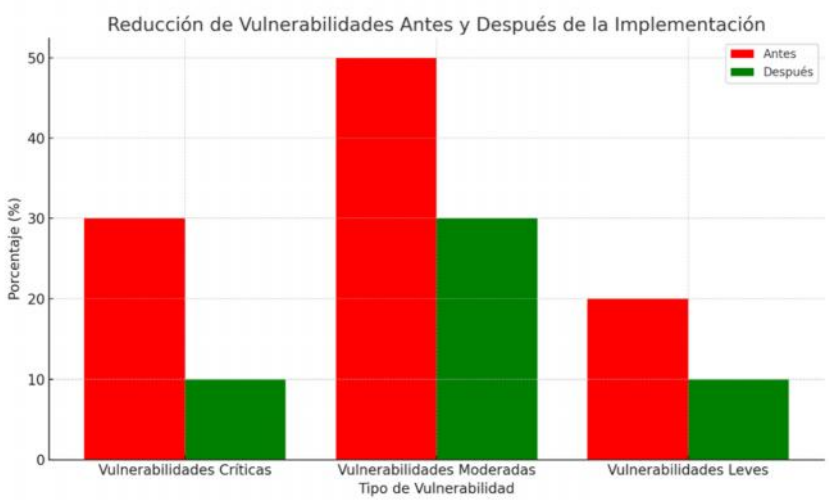
HP Inc. (2020). *Guía de creación de informes HP TechPulse*. https://ftp.hp.com/pub/caps-softpaq/HP_DaaS/Documentation/Welcome_Kit/User_Guides/HP_TechPulse_Reporting_Guide-ES.pdf

Microsoft. (2025, 13 de febrero). *Implementación de la infraestructura de identidad para Microsoft 365*. Microsoft Learn. https://learn.microsoft.com/es-es/microsoft-365/enterprise/deploy-identity-solution-overview?view=o365-worldwide

7. ANEXOS

Figura 1 Comparación de Vulnerabilidades del antes y después el realizar las mejoras de las vulnerabilidades.

Figura 1 Comparación de Vulnerabilidades del antes y después el realizar las mejoras de las vulnerabilidades.



Nota.

Figura 2 Dashboard de Red, clientes enlaces y consumo de red

Figura 2 Dashboard de Red, clientes enlaces y consumo de red

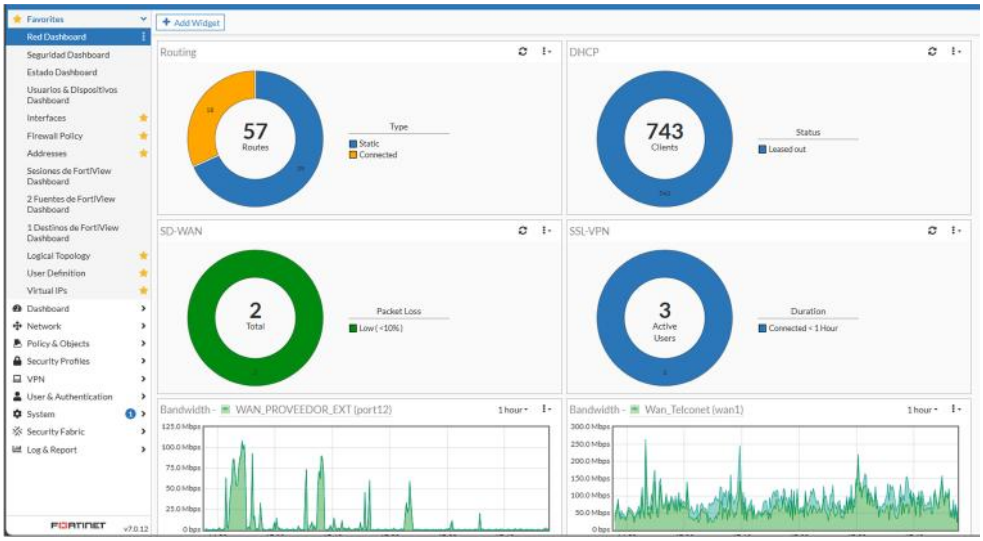


Figura 3. Total de dispositivos detectados y conectados en la red.

Figura 3 Total de dispositivos detectados y conectados en la red.

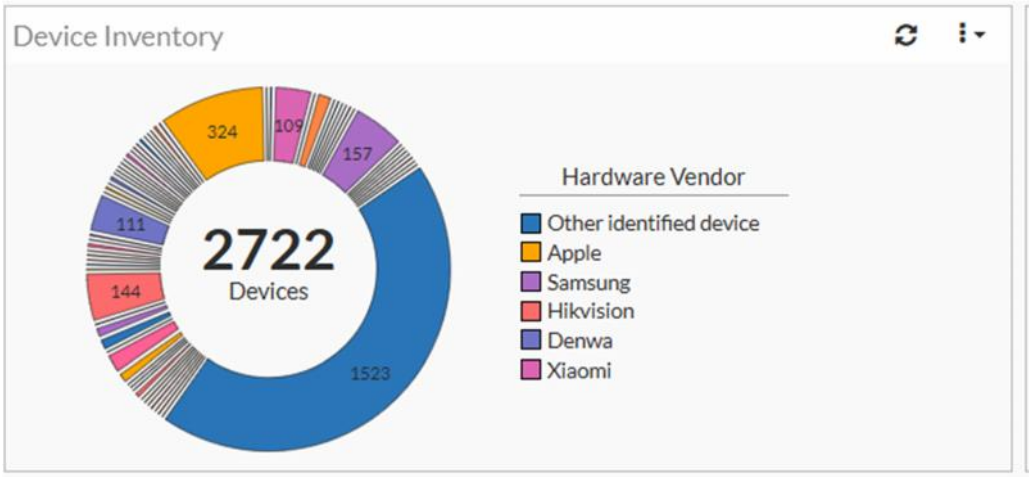


Figura 4 Dashboard Hp Tech Pulse , semaforización de Vulnerabilidades en equipos de usuarios.

Figura 4 Dashboard Hp Tech Pulse , semaforización de Vulnerabilidades en equipos de usuarios.

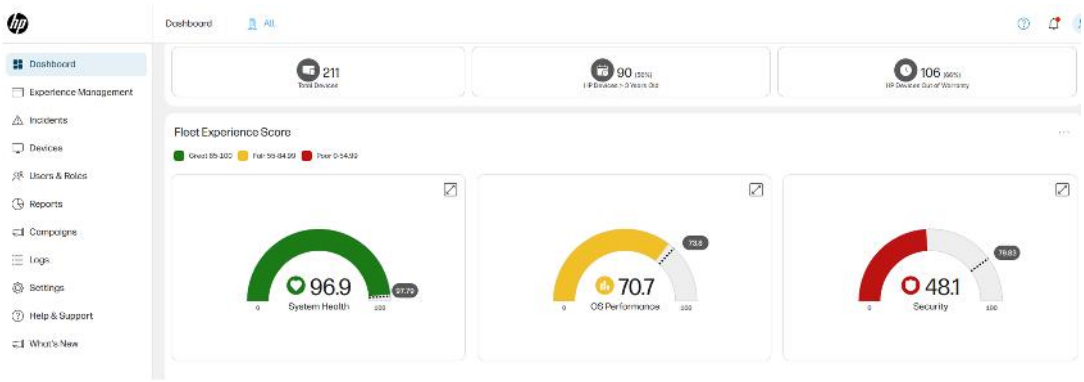


Figura 5 Score de Seguridad en equipos de Usuarios

Figura 5 Score de Seguridad en equipos de Usuarios

Figura 6 Top 5 de los índices más altos encontrados en la compañía

Figura 6 Top 5 de los índices más altos encontrados en la compañía

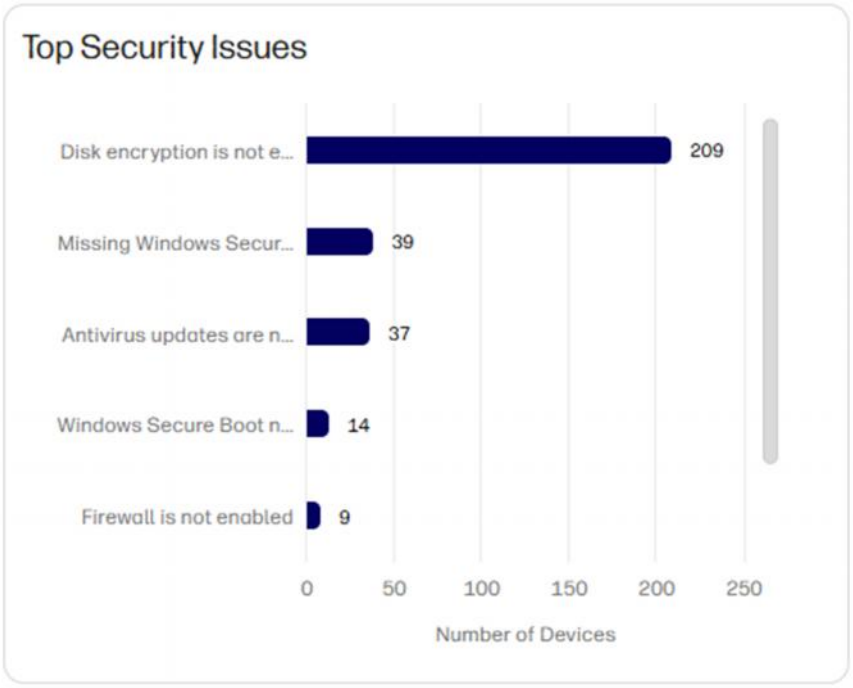


Figura 7 Acciones a recomendar.

Figura 7 Acciones a recomendar.

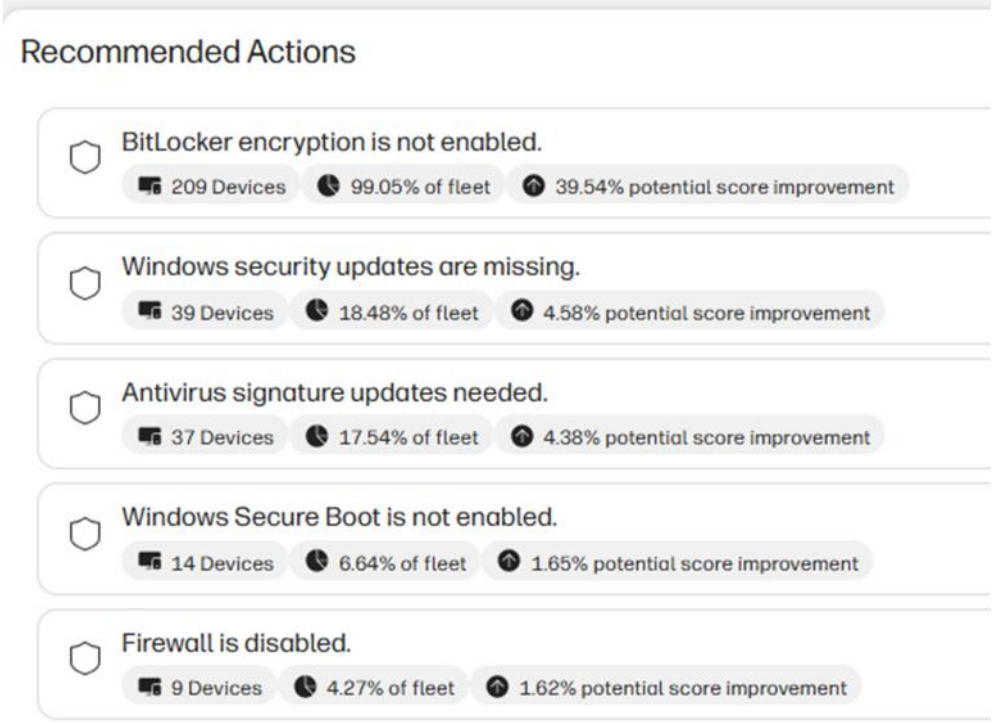


Figura 8 Plataforma de Monitoreo de Consumo de Internet Corporativo

Figura 8 Plataforma de Monitoreo de Consumo de Internet Corporativo

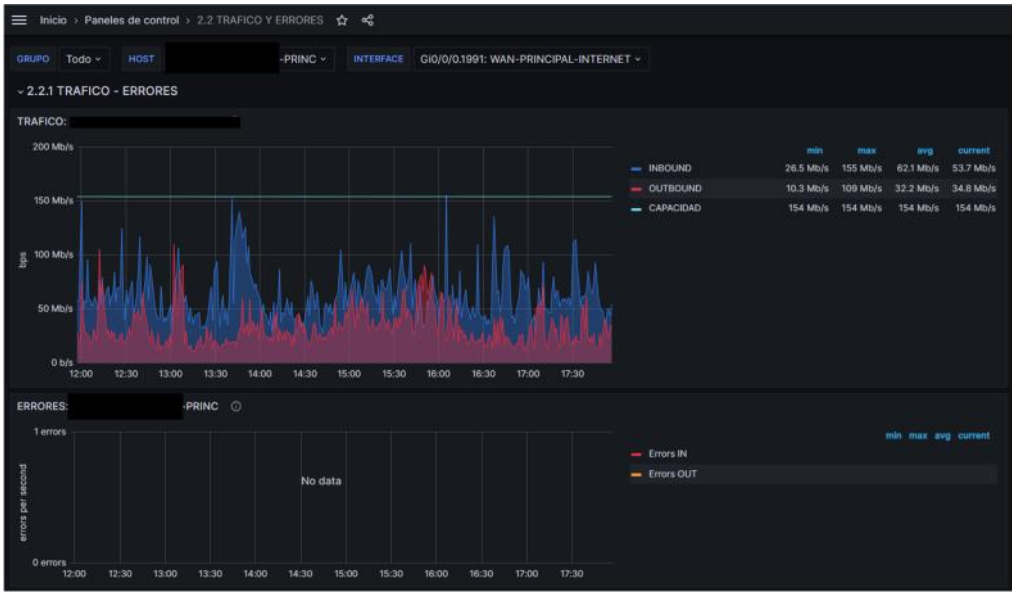


Figura 9 Plataforma de Monitoreo de Consumo de Lans Corporativo

Figura 9 Plataforma de Monitoreo de Consumo de Lans Corporativo

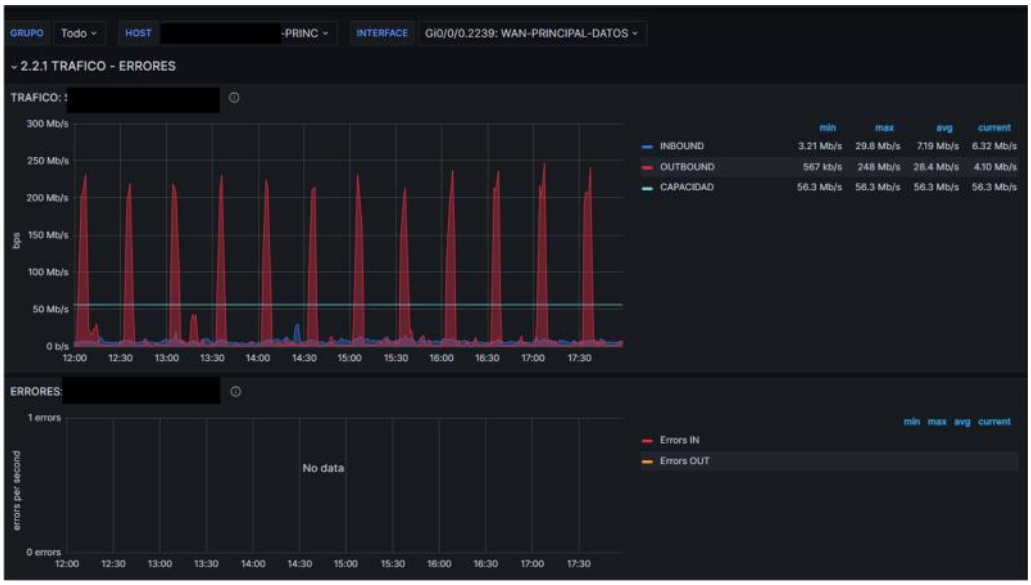


Figura 10 Dispositivos registrados en Plataforma Identidad Microsoft Azure

Figura 10 Dispositivos registrados en Plataforma Identidad Microsoft Azure

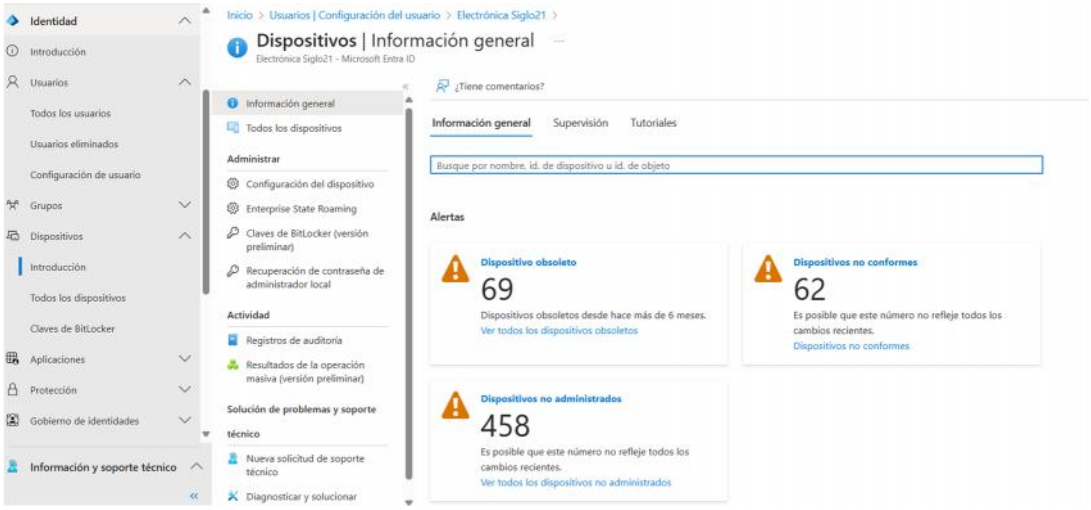


Figura 11 Plataforma de Antivirus Indicando las vulnerabilidades presentadas

Figura 11 Plataforma de Antivirus Indicando las vulnerabilidades presentadas

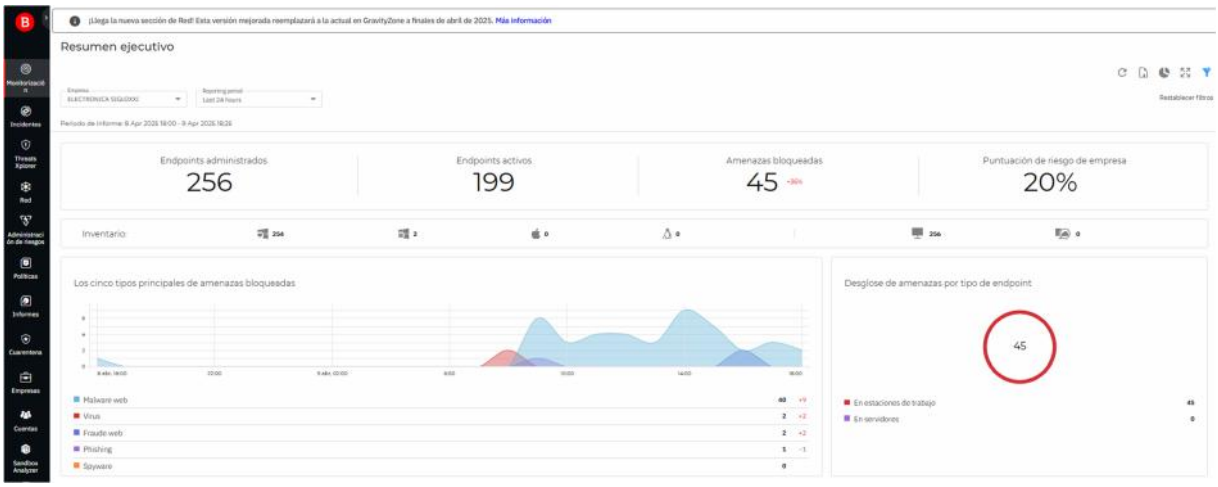


Figura 12 Plataforma de Antivirus Score de mayor ataque registrado en las ultimas horas

Figura 12 Plataforma de Antivirus Score de mayor ataque registrado en las ultimas horas

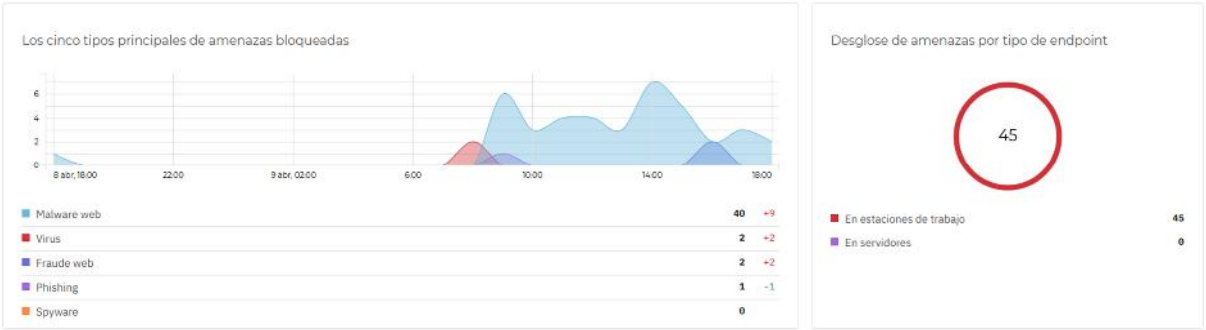


Figura 13 Plataforma de Antivirus indicando las acciones tomadas

Figura 13 Plataforma de Antivirus indicando las acciones tomadas

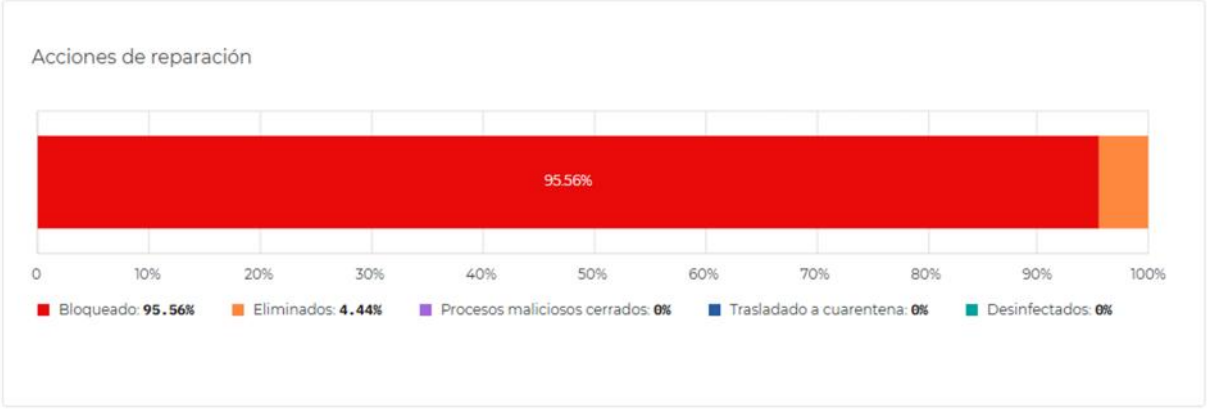


Figura 14 Plataforma de Antivirus Módulos Endpoint por Usuario

Figura 14 Plataforma de Antivirus Módulos Endpoint por Usuario

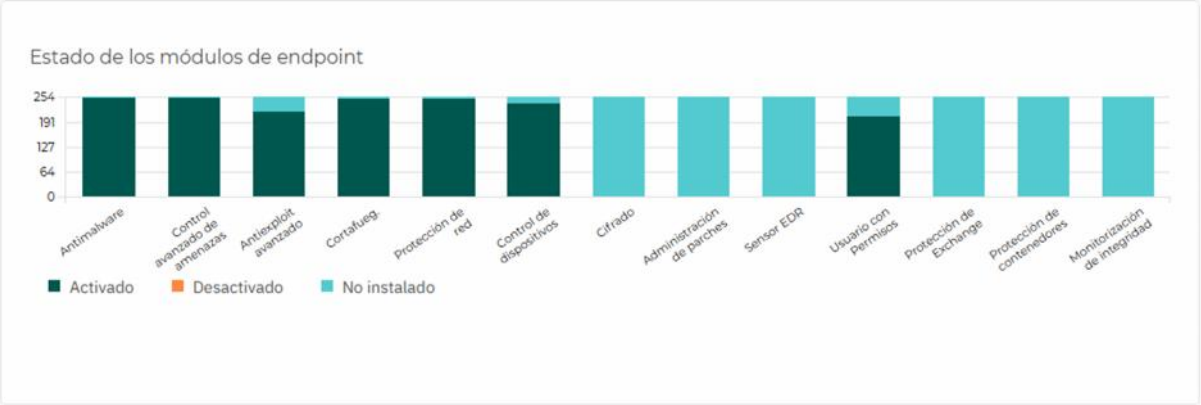


Figura 15 Plataforma de Antivirus Auditoria de Seguridad por equipos

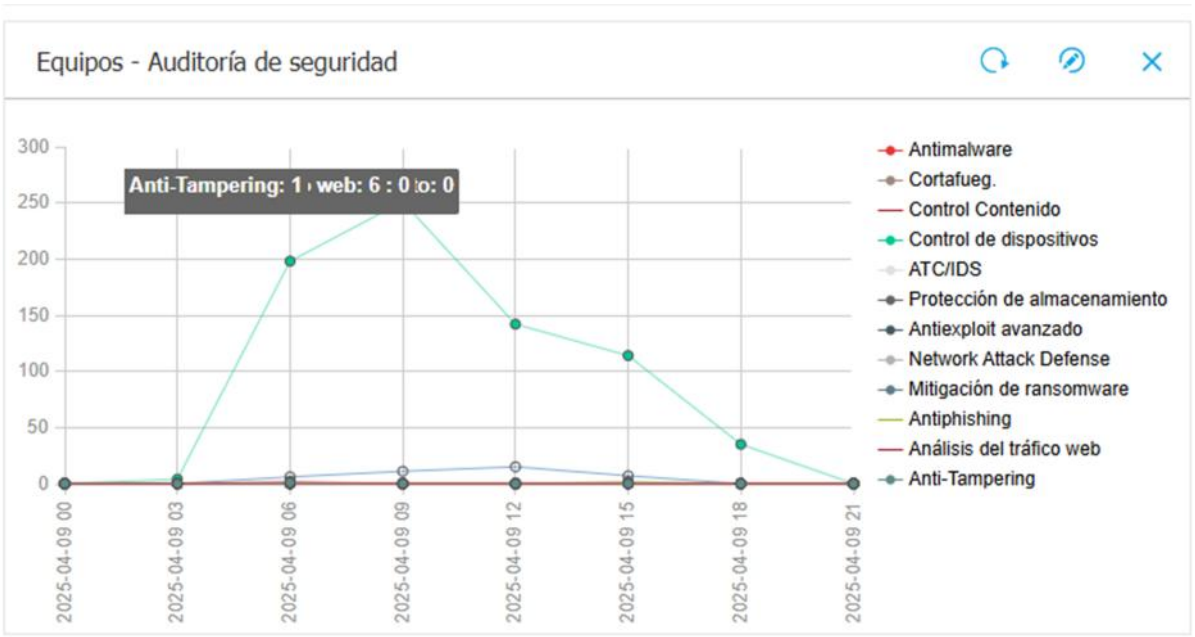



Figura 15 Plataforma de Antivirus Auditoria de Seguridad por equipos