Mejores prácticas de Seguridad en la Infraestructura de Red en Preflex S.A.S e Identificación de Vulnerabilidades

Duvan Felipe Piñeros Chacon, Andrés Felipe Estrada Padilla, Andrea Carolina Jimenes Portilla y Karen Daniela Casasbuenas Torres

Especialización en Seguridad Informática, Fundación Universitaria Compensar

Seminario de Grado

Jaime Andrés Chaparro Sánchez

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional

Resumen

El presente documento de consultoría busca reforzar la seguridad de la infraestructura de red de Preflex S.A.S Haciendo enfoque en firewalls, servidores on-premise y switches, la evaluación inicial aborda la arquitectura de red para identificar y detectar posibles vulnerabilidades; se buscarán puntos a mejorar como políticas de firewall y la implementación del mismo acordes a la necesidad de la empresa para optimizar las reglas de una protección efectiva; ahora bien el presente proyecto de consultoría pretende mejorar la seguridad de los servidores mediante el proceso de hardening, así mismo se llevará a cabo una revisión de las configuraciones actuales de los switches para identificar y corregir vulnerabilidades.

El proyecto concluirá con la entrega de documentación detallada de configuraciones y cambios, informes de evaluación de la infraestructura, es relevante señalar que se dispone de documentación y detalles específicos sobre la infraestructura actual de Preflex S.A.S En resumen, el proyecto aborda los desafíos de seguridad desde múltiples ángulos, asegurando una infraestructura robusta y resistente a posibles amenazas. (mencionar el tema económico, en cuanto a las implementaciones como por ejemplo el firewall acorde a la escalabilidad de la empresa)

Palabras clave: hardening, seguridad de red, firewall, servidores on-premise, switches, evaluación de vulnerabilidades.

Abstract

This consulting document aims to reinforce the security of PREFELX S.A.S.'s network infrastructure. Focusing on firewalls, on-premise servers, and switches, the initial assessment addresses the network architecture to identify and detect potential vulnerabilities. We will search for areas to improve such as firewall policies and its implementation in line with the company's needs to optimize the rules for effective protection. Additionally, this consulting project aims to enhance server security through hardening methodologies. A review of current switch configurations will also be carried out to identify and correct vulnerabilities.

The project will conclude with the delivery of detailed documentation of configurations and changes, along with infrastructure assessment reports. It is worth noting that specific documentation and details about Preflex S.A.S current infrastructure are available. In summary, the project addresses security challenges from multiple angles, ensuring a robust infrastructure resistant to potential threats.

Keywords: hardening, network security, firewall, on-premise servers, switches, vulnerability assessment.

Tabla de Contenido

1. MARCO TEÓRICO 7

1.1 REDES DE COMPUTADORAS 7
1.2 HARDENING 8

2. DISEÑO METODOLÓGICO 9

3. RESULTADOS ESPERADOS 11

4. CONCLUSIONES Y RECOMENDACIONES 14

4.1 CONCLUSIONES 14
4.2 RECOMENDACIONES 14

Introducción

El presente documento tiene como propósito dar a conocer una estrategia de Hardening para los equipos firewall, switches y servidores On-premise de la empresa Preflex S.A.S Tras una investigación, se ha identificado que estos equipos actualmente están obsoletos afectando la seguridad y el rendimiento de la empresa. En respuesta a este desafío, se busca planear un diseño en el cual se pueda actualizar el hardware, y políticas según la necesidad de la empresa a un costo que se ajuste a las actividades e ingresos de la empresa. El propósito final es proteger los activos de la información de Preflex S.A.S de manera efectiva y preparar la red para el crecimiento continuo de la empresa.

Las investigaciones de los últimos años muestran los cambios en las amenazas cibernéticas que subrayan una realidad crítica, los ciberdelincuentes están diversificando y actualizando sus tácticas, lo que revela que ningún sector queda exento de riesgos. Se confirmó que hay más de 2.200 ciberataques al día, eso equivale a más de 800.000 ataques cada año, según la la revista de Security.

En Estados Unidos, una filtración de datos cuesta una media de 9,44 millones de dólares y se prevé que el ciberdelito cueste 8 billones de dólares en 2023.

Información Tomada de, Jain, S. (2024, 8 febrero). 160 Cybersecurity Statistics: Updated Report 2024. Astra Security Blog. https://www.getastra.com/blog/security-audit/cyber-security-statistics/

Se prevé que la ciberdelincuencia le cueste al mundo 9,5 billones de dólares en 2024 y se espera que los costes globales de los daños causados por la ciberdelincuencia crezcan un 15% anual durante los próximos dos años, alcanzando los 10,5 billones de dólares anuales en 2025.

Fox, J. (2023, December 8). Top Cybersecurity Statistics for 2024. Www.cobalt.io. https://www.cobalt.io/blog/cybersecurity-statistics-2024

El presente trabajo pretende el aseguramiento de la información mediante actualizaciones de Hardware necesarias que permitan administrar los datos importantes. Esto implicará la identificación, evaluación y mitigación de posibles riesgos de seguridad que puedan comprometer la integridad, confidencialidad y disponibilidad de los sistemas de información de Preflex S.A.S

El resultado esperado será la recomendación correcta para la infraestructura de red más robusta y segura, capaz de soportar el crecimiento continuo de la empresa y proteger sus activos de información de manera efectiva.

Antecedentes y Justificación

Las organizaciones enfrentan constantes intentos de vulneración por parte de la delincuencia informática. Preflex S.A.S no es la excepción, se trata de una empresa que tiene bastantes debilidades y es muy apta para sufrir cualquier tipo de ataque por la forma que está administrada a nivel de infraestructura tecnológica. El objetivo de los delincuentes y ciberataques siempre es obtener información confidencial, robarla o secuestrarla lo que representa una amenaza significativa para la seguridad de la información de la empresa. En la actualidad, las víctimas de estos ataques son cada vez más frecuentes, afectando a empresas de todos los tamaños, desde grandes corporaciones hasta pequeñas y medianas empresas.

Estos ataques suelen dirigirse a la infraestructura de la empresa, especialmente cuando la capacitación del personal, la adquisición de equipos adecuados y la implementación de medidas de seguridad no han sido prioridades.

Preflex S.A.S es una empresa que lleva en el mercado 39 años, dedicada a la fabricación y venta de Polímeros para pinturas, adhesivos para empaques, auxiliares y resinas para textiles, adhesivos para madera, cementos de contacto para la industria, sustratos para impresión a gran formato e insumos para artes gráficas.

Está constituida por 500 empleados, en las áreas de comercial, recursos humanos, servicio al cliente, gerencia, tecnología y operaciones.

Para este proyecto se tienen todas las áreas en cuenta frente al funcionamiento, pero se hace énfasis en TI, ya que es la directamente relacionada con la seguridad de la información.

En cuanto a infraestructura se tienen seis switches, tres servidores On-premise con sistema operativo Windows Server 2008, Windows Server 2019 y Windows 7. Dos equipos Firewall, un D-link y un Fortinet, donde únicamente se administra las VPN Cliente ya que no tiene licenciamiento y se usa desde lo Free que permite trabajar.

IDENTIFICADOR	MARCA	REFERENCIA	Administrado
SW-1	TP-Link	TL-SG1024D	NO
SW-2	TP-Link	TL-SG1024D	NO
SW-CORE1	TP-Link	TL-SG3452 V1.20	SI
SW-3	D-Link	DES-3028	NO
SW-4	TP-Link	TL-SG3428 v1.0	SI
SW-5	TP-Link	TL-SG1024	NO
SW-CORE2	TP-Link	TL-SG3428 v1.0	SI
FW	D-Link	DFL-860E	SI
FW-VPN	FORTINET	Fortigate 300D	SI

Tabla 1. Equipos Preflex SAS

Tabla1: Según el análisis se evidencia que los equipos a nivel tecnológico están muy desactualizados lo que genera múltiples vulnerabilidades. A raíz de esto se harán las sugerencias pertinentes para mejorar la seguridad de los equipos mencionados.

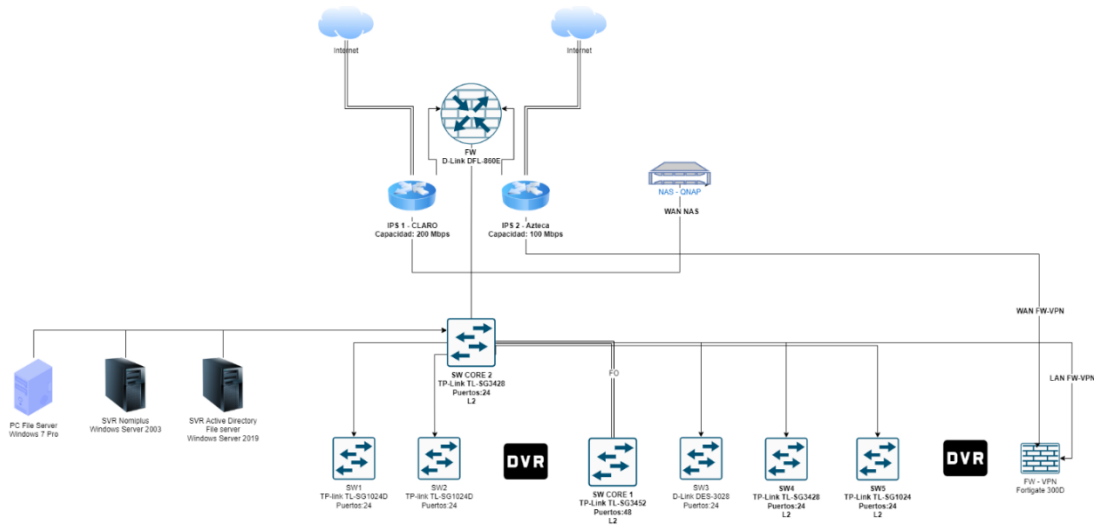


Ilustración 1. Topología Preflex SAS

Formulación del Problema

La infraestructura de red de Preflex S.A.S se enfrenta a desafíos importantes en cuanto a seguridad, evidenciados por posibles vulnerabilidades en sus firewalls, servidores on-premise y switches. Estas vulnerabilidades plantean riesgos significativos para la integridad de los datos, la continuidad operativa y la confidencialidad de la información crítica. Se requiere una evaluación exhaustiva para identificar y abordar estas vulnerabilidades, asegurando así una infraestructura de red robusta y segura para Preflex S.A.S

¿Cómo puede Preflex S.A.S desarrollar un enfoque que evalúe y mejore la seguridad de su infraestructura de red, abordando la identificación y mitigación de vulnerabilidades en firewalls, servidores on-premise y switches?

Objetivo General

Identificar los fallos, vulnerabilidades y necesidades de seguridad en la infraestructura on-premise dentro de la empresa Preflex S.A.S

Objetivos Específicos

- Detectar las vulnerabilidades que presenta la infraestructura de la empresa Preflex S.A.S mediante la herramienta Nessus de Tanable.
- Evaluar posibles soluciones basadas en el proceso de Hardening para los equipos de tecnología, priorizando aquellas que ofrecen el mejor equilibrio entre costo y beneficio.
- Proponer una estrategia de actualización a la infraestructura enfocada al firewall y servidores On-Premise, que garantice la seguridad de los datos y esté al alcance económico de la empresa

Alcances y Limitaciones

El alcance de este proyecto abarca una evaluación integral de la infraestructura de red de Preflex S.A.S para identificar posibles vulnerabilidades en firewalls, servidores on-premise y switches, seguido por estrategias para fortalecer la seguridad de la red. Las actividades incluirán soluciones propuestas, así como la elaboración de documentación detallada de los hallazgos y recomendaciones. Las limitaciones incluyen recursos limitados en términos de tiempo, personal y presupuesto, así como el alcance tecnológico restringido a la infraestructura de red de Preflex S.A.S y la dependencia de factores externos como la disponibilidad de terceros proveedores

1. Marco teórico

Teniendo en consideración que el enfoque principal del presente proyecto abraca el análisis de vulnerabilidades y el nombramiento de las características necesarias para robustecer ciertos componentes de la infraestructura de red de una organización, es oportuno mencionar la importancia que tiene la ejecución de las buenas prácticas en los procesos de implementación de redes informáticas; las cuales se basan en conocimientos fundamentales de ciertos conceptos teóricos y técnicos. Dicho esto, se trae a colación algunos criterios pertenecientes al marco referencial del planteamiento en mención.

1.1 Redes de computadoras

Los desarrollos informáticos dominaron los avances tecnológicos del siglo XX para la humanidad; en ese periodo se buscó abarcar la recolección, transporte, almacenamiento y el tratamiento adecuado para la información digital. El procesamiento de datos a través de computadoras robustas en tamaño, pero limitadas en capacidad quedó atrás para dar paso a sistemas altamente capacitados para proveer un procesamiento de carga exponencial a comparación del permitido hace seis décadas atrás. Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de Computadoras (5th ed.). Pearson.

El vertiginoso crecimiento de la industria de la computación en el siglo XXI se traduce en la producción de miles de millones de computadoras mucho menor en tamaño, pero con una capacidad de procesamiento altamente superior en comparación a los sistemas en uso de hace cinco décadas. De la mano, la industria ha tenido avances espectaculares en conceptos relacionados a diseños de redes de datos, desde topologías de alto rendimiento hasta arquitecturas administradas lógicamente como es el ejemplo de los servicios Cloud. Kurose, J. F., & Ross, K. W. (2016). Redes de Computadoras: Un enfoque descendente (7th ed.). Pearson.

1.2 Hardening

La concepción de la informática trajo consigo el concepto de interconexión, la idea de compartir información a través de una extensa red era parte del proceso de globalización que tanto deseaban alcanzar los pioneros en la implementación de las arquitecturas de redes durante sus primeros años. Hoy en día la red de redes, Internet, tiene millones de millones de usuarios que hacen uso de una infinidad de recursos tales como plataformas para realizar transacciones electrónicas, compras en línea, almacenamiento de información privada entre otros, de la misma forma cada día se detectan más vulnerabilidades, convirtiendo así la seguridad informática en un problema de alta prioridad para los usuarios finales y los gestores que supervisan y administran estos recursos. Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Pearson.

El hardening, traducido al español como "endurecimiento" es el proceso en el cual se refuerza la seguridad de un sistema informático a través de la implementación de medidas que minimizan amenazas latentes y reducen las posibles áreas de ataque y vulnerabilidad, todo ello con base a conceptos teóricos, citando a Tanenbaum en su libro Redes de Computadoras "Los problemas de seguridad de las redes se pueden dividir en términos generales en cuatro áreas interrelacionadas: confidencialidad, autentificación, no repudio y control de integridad." (Tanenbaum & Wetherall, 1981).

El endurecimiento abarca diferentes medidas que pueden implementarse como el descarte de servicios innecesarios, validación de reglas de seguridad, actualizaciones a dispositivos perimetrales entre otros, siempre teniendo en cuenta el objetivo principal; reducir las posibilidades de recibir ataques de agentes maliciosos internos o externos y aumentar los niveles de confiabilidad y resiliencia, citando nuevamente a Tanenbaum, "hacer segura una red comprende mucho más que simplemente mantenerla libre de errores de programación. Implica ser más listo que adversarios a menudo inteligentes, dedicados y a veces bien financiados" (Tanenbaum & Wetherall, 1981).

2. Diseño Metodológico

El proyecto de consultoría de hardening de red para Preflex S.A.S se estructura en tres etapas esenciales, diseñadas para fortalecer la seguridad de su infraestructura interna. La primera fase, el Reconocimiento, inicia con una revisión detallada de servidores on-premise, switches (de acceso y core), y firewalls. Su objetivo es identificar posibles puntos débiles y vulnerabilidades que puedan afectar la seguridad de la red, para lo cual se usará una herramienta de escaneo de vulnerabilidades llamada Nessus.

Posteriormente, la Etapa de Diagnóstico implica una evaluación técnica de servidores, verificando sistemas operativos en busca de vulnerabilidades conocidas y riesgos asociados. Se realiza un análisis de las especificaciones de los switches, determinando la viabilidad de mejorar la configuración existente o recomendar su sustitución. Durante esta etapa, se revisarán las reglas de seguridad existentes, garantizando una configuración óptima y evaluando características clave como la alta disponibilidad.

Finalmente, la Etapa de Resultados y Documentación presentará los hallazgos de los respectivos escaneos. Las vulnerabilidades encontradas y las medidas de hardening que puedan ser aplicadas. Asimismo, para los equipos Firewall y oportunidades de mejora que aporten al fortalecimiento de la seguridad perimetral de Preflex S.A.S.

3. Resultados esperados

Para la etapa de resultados, se generó los escaneos para los equipos de Preflex S.A.S utilizando la herramienta Nessus de Tenable la cual encontró la siguiente información.

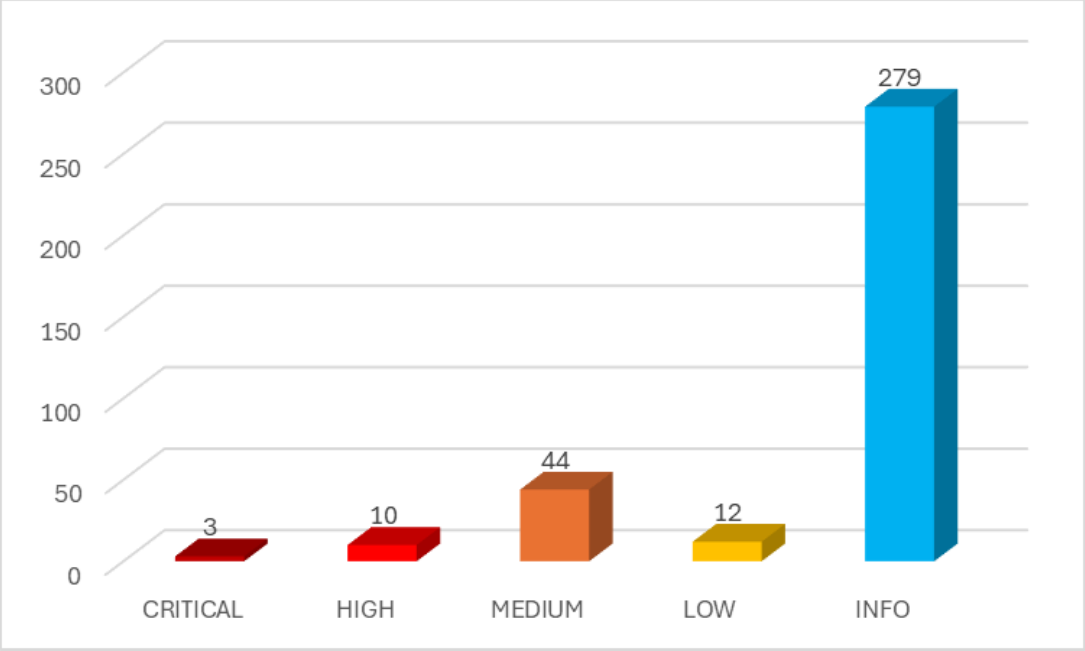


Ilustración 2. Vulnerabilidades encontradas por impacto.

En la ilustración2, se muestra el resultado en números enteros de las vulnerabilidades halladas de manera global en todos los equipos escaneados discriminados en la criticidad de las vulnerabilidades basadas en la clasificación de CVE obtenida en la herramienta Nessus, es importante considerar el porcentaje que representa cada clasificación

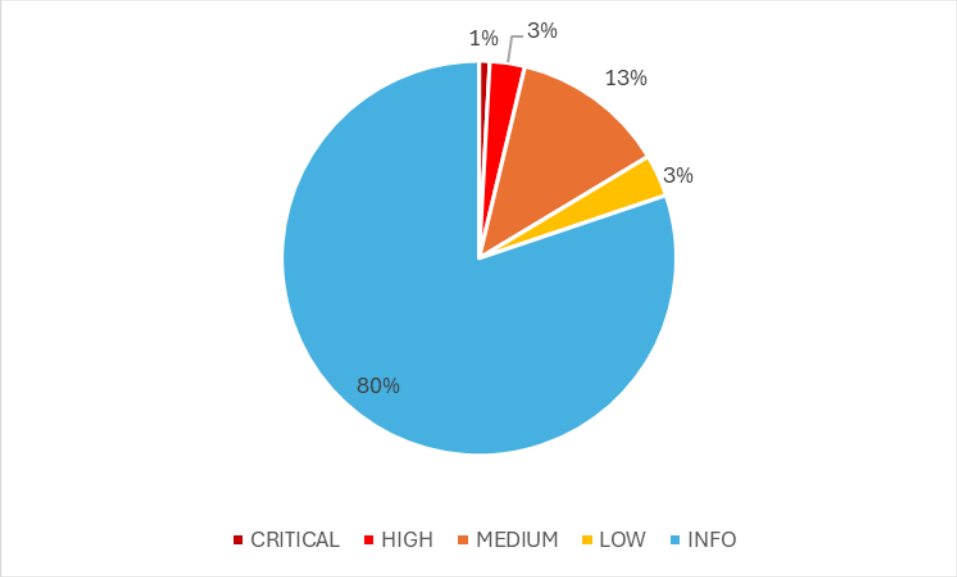


Ilustración 3. Clasificación de Vulnerabilidades.

Detección vulnerabilidades de impacto critico: Dando enfoque a las vulnerabilidades críticas con score CVSS3 superior a 9.0 se evidencia la siguiente información en el equipo SVR Nomiplus, a continuación, se describen y se relaciona una posible solución.

- **Detección de protocolos SSL versión 2 y 3**

Descripción: El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varios fallos criptográficos.

Solución: Consulte la documentación de la aplicación para desactivar SSL 2.0 y 3.0. En su lugar, utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior.

- **Detección de versiones no admitidas de Microsoft SQL Server (comprobación remota)**

Descripción: De acuerdo con su número de versión auto informado, ya no se admite la instalación de Microsoft SQL Server en el host remoto.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución: Actualice a una versión de Microsoft SQL Server que sea compatible actualmente.

- **Sistema operativo Windows no compatible (remoto)**

Descripción: A la versión remota de Microsoft Windows le falta un Service Pack o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad.
Solución: Actualizar a un Service Pack o sistema operativo compatible.

Detección vulnerabilidades de impacto Alto:

En cuanto al impacto en la categoría Alto, se identificaron 10 vulnerabilidades importantes para tratar de forma prioritaria. La evaluación de seguridad reveló que algunos certificados SSL en la cadena emplean algoritmos hash débiles, lo que compromete la integridad del cifrado.
Adicional, se descubrió que es posible acceder a recursos compartidos de red sin. Asimismo, ciertos servicios remotos permiten el uso de cifrados SSL de potencia media, debilitando la protección de las comunicaciones.
Adicional revelo que el host remoto de Windows está afectado por múltiples vulnerabilidades y es vulnerable a la elevación de privilegios mediante reflexión NTLM. Se identificó la posibilidad de iniciar sesión en el host remoto utilizando una sesión NULL, lo cual representa un riesgo significativo. Por último, se constató que algunos servicios remotos ofrecen protocolos criptográficos inseguros, incrementando la exposición a potenciales ataques.
NOTA: Para relacionar la demás vulnerabilidad según los impactos Alto, medio, bajo e informativo se detallan en los anexos del 01 al 09.

4. Conclusiones y recomendaciones

4.1 Conclusiones

- El uso de la herramienta NESUS ha sido fundamental, ya que permitió una visión clara y precisa del estado de los dispositivos de red mediante el escaneo de vulnerabilidades. Este paso hace parte de la fase inicial, para comprender las condiciones actuales de la infraestructura de red, para identificar fallos de seguridad y debilidades.
- Con el conocimiento del estado actual, la finalidad es conocer y con base a este poder mejorar proporcionando una base sólida para implementar medidas de seguridad más robustas, así la empresa puede fortalecer su infraestructura asegurando la protección continua de sus datos y manteniendo un entorno digital más seguro y resiliente.
- Contar con equipos que cumplan con las necesidades específicas de la empresa y que sean administrables es indispensable para mantener un entorno seguro y protegido contra las amenazas en constante evolución.
- En la actualidad, las amenazas y los ciberdelincuentes están siempre a la vanguardia, mejorando y actualizando constantemente sus técnicas. Por ello, es fundamental dar prioridad e importancia a la seguridad de la información.

4.2 Recomendaciones

- Realizar la revisión detallada de los escaneos ejecutados verificando cada vulnerabilidad en cada equipo para generar un plan de mitigación que aborde las vulnerabilidades presentadas en los Anexos del 01 al 09.

- Implementar infraestructura redundante o de contingencia que busque mitigar el impacto en caso de una posible afectación a la infraestructura física de Preflex S.A.S apuntando a la continuidad del negocio; incorporando equipos de respaldo basados en la norma ISO 27031 de 2011.
- Invertir en tecnologías de vanguardia a nivel de seguridad perimetral, incluyendo un NGFW en un esquema Activo/Pasivo integrando funcionalidades de inspección detallada de tráfico, VPNs Client to Site, VPNs Site to Site, algoritmos de cifrado robustos y actuales, URL Filtering. Esto debido a que el Firewall actual de Preflex S.A.S no cuenta con la mayoría de estas funcionalidades o son muy limitadas y que están descritas en el datasheet del producto.
- Para optimizar la infraestructura de TI de Preflex S.A.S. en cuanto a servidores mostrada en Ilustración 2: Topología Preflex S.A.S, se recomienda implementar un servidor de respaldo para el "SVR Active Directory File Server" con un proveedor diferente al actual, garantizando así la mitigación de riesgos. Además, se sugiere utilizar sistemas de monitoreo y respaldo como Nagios ó VMware para la gestión y automatización de copias de respaldo. Es esencial que todos los servidores y software sean de versiones 2019 o más recientes para asegurar soporte y actualizaciones adecuadas, minimizando los riesgos de seguridad y funcionalidad asociados con versiones anteriores.
- Teniendo en cuenta el planteamiento del problema y el análisis realizado, podemos concluir que la infraestructura de red de la organización requiere de ciertas actualizaciones con base a sus necesidades actuales; las cuales contemplan el correcto dimensionamiento de una posible implementación. Respecto a la seguridad perimetral. El Firewall D-Link DFL-860E actualmente en uso ha llegado al fin de su soporte. Por lo cual se podrían tener en consideración las siguientes características a la hora de implementar un dispositivo de seguridad perimetral.

CARACTERISTICA	DESCRIPCIÓN
Despliegue de Sistema Operativo	Appliance, Virtual, Hosted, Cloud

Capacidad de Alta Disponibilidad	Activo-Activo Activo-Pasivo Clustering
Servicios	Seguridad web Seguridad de contenido Seguridad de dispositivos
Procesador	SPU (Security Processing Unit) Capacidad superior (520Gbps) para detectar amenazas y bloquearlas sin afectar la seguridad de red.
Fuente de alimentación dual	Redundancia, no intercambiables en caliente.

Tabla 2. Características y descripciones, seguridad perimetral

Bibliografía

- Información Tomada de, Jain, S. (2024, 8 febrero). 160 Cybersecurity Statistics: Updated Report 2024. Astra Security Blog. https://www.getastra.com/blog/security-audit/cyber-security-statistics/
- Fox, J. (2023, December 8). Top Cybersecurity Statistics for 2024. Www.cobalt.io. https://www.cobalt.io/blog/cybersecurity-statistics-2024
- Tanenbaum, A. S., & Wetherall, D. J. (2011). Redes de Computadoras (5th ed.). Pearson.
- servicios Cloud. Kurose, J. F., & Ross, K. W. (2016). Redes de Computadoras: Un enfoque descendente (7th ed.). Pearson.
- Pfleeger, C. P., & Pfleeger, S. L. (2015). Security in Computing (5th ed.). Pearson.
- “Los problemas de seguridad de las redes se pueden dividir en términos generales en cuatro áreas interrelacionadas: confidencialidad, autentificación, no repudio y control de integridad.” (Tanenbaum & Wetherall, 1981).
- “hacer segura una red comprende mucho más que simplemente mantenerla libre de errores de programación. Implica ser más listo que adversarios a menudo inteligentes, dedicados y a veces bien financiados” (Tanenbaum & Wetherall, 1981).