UNIVERSIDAD POLITÉCNICA SALESIANA ECUADOR

POSGRADOS

MAESTRÍA EN
SEGURIDAD DE LA INFORMACIÓN
RPC-SO-28-NO.669-2021

OPCIÓN DE TITULACIÓN:

PROYECTO DE TITULACIÓN CON COMPONENTES DE INVESTIGACIÓN APLICADA Y/O DE DESARROLLO

TEMA:

ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA SEGUROS ALIANZA S.A.

AUTOR:

LUIS GUSTAVO SÁNCHEZ CAIZA

DIRECTOR:

JUAN CARLOS DOMÍNGUEZ AYALA

CUENCA – ECUADOR
2024

Autor:

Luis Gustavo Sánchez Caiza
Ingeniero en Sistemas de Información.
Candidato a Magíster en Seguridad de la Información por la Universidad Politécnica Salesiana – Sede Cuenca.
lsanchezc7@est.ups.edu.ec

Dirigido por:

Juan Carlos Domínguez Ayala
Ingeniero de Sistemas.
Magister en Redes de Comunicaciones.
jdominguez@ups.edu.ec

DEDICATORIA

Deseo dedicar este trabajo de titulación a mi familia, en especial a mi querida madre, quien ha estado a mi lado brindándome un apoyo incondicional a lo largo de todo este proceso. También quiero reconocer a mi padre, cuyos consejos, motivación y ejemplo han sido fundamentales en mi desarrollo académico. Agradezco a mi hermana, sobrinos, esposa e hija por su constante apoyo y comprensión durante mi trayectoria en esta maestría. El respaldo de todas estas personas, que son mi mundo y mi mayor fuente de inspiración, ha sido crucial para lograr culminar esta etapa importante en mi vida profesional.

Gustavo

AGRADECIMIENTO

Quiero expresar mi profundo agradecimiento a Dios por haberme brindado la oportunidad de realizar esta maestría, la cual tiene un significado invaluable tanto en mi desarrollo profesional como personal. Me llena de satisfacción y orgullo haber completado este importante logro en mi vida.

Asimismo, deseo agradecer de manera especial a mi madre y padre, quienes han desempeñado un papel fundamental en mi crecimiento y desarrollo a lo largo de los años. Su incondicional apoyo, guía y amor han sido pilares fundamentales en mi formación y éxito académico. Sin ellos, no habría sido posible alcanzar esta meta.

No puedo dejar de mencionar mi agradecimiento a todos los maestros y autoridades de la Universidad Politécnica Salesiana. Su dedicación, esfuerzo y valiosos conocimientos impartidos a lo largo de todo el proceso de formación de la maestría han sido fundamentales para mi aprendizaje y crecimiento profesional.

Gustavo

Tabla de Contenido

ANÁLISIS DE LA CIBERSEGURIDAD A LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA SEGUROS ALIANZA S.A.

AUTOR(ES):

LUIS GUSTAVO SÁNCHEZ CAIZA

RESUMEN

El presente documento de titulación tiene como propósito llevar a cabo la implementación de un mecanismo u herramienta de seguridad que permita analizar, detectar y filtrar posibles indicios de ataques cibernéticos hacia las aplicaciones web que son desarrolladas internamente en la empresa Seguros Alianza S.A.

La importancia de dicha finalidad radica en que actualmente los ataques cibernéticos tienen como objetivos varios objetivos dentro de una infraestructura tecnológica corporativa como por ejemplo el servidor donde se encuentran alojadas las aplicaciones web que poseen las organizaciones, con las cuales se realizan las gestiones y operaciones para la administración, productividad y continuidad del negocio, así como también la automatización de los procesos internos y externos.

En la mayoría de los casos no existe un control o una política de seguridad para el desarrollo de aplicaciones web seguras, puesto que los desarrolladores desconocen de una metodología que les permita generar un código que sea seguro o a su vez por factores de tiempo o plazos que se establecen en los proyectos los cuales se los deben cumplir hacen que los desarrolladores se enfoquen más la funcionalidad de las aplicaciones web que en la seguridad de estas.

Una mala práctica en el desarrollo de aplicaciones web, así como el no darle la importancia del caso a la seguridad tendrían consecuencias que podrían llegar a ser extremadamente graves debido a los datos sensibles que tienen los usuarios, puesto que se ingresan datos personales, datos bancarios y demás información que podría llegar a ser vulnerada por un delincuente informático generando un riesgo alto para la organización.

De tal manera que en el entorno organizacional se vuelve indispensable obtener o implementar un mecanismo que proporcione una seguridad adicional para las aplicaciones web y que la responsabilidad de la seguridad no recaiga sobre el desarrollador sino más bien que se pueda tener un filtro inteligente y automatizado

que permita realizar detecciones de ataques hacia nuestras aplicaciones web como un WAF (Cortafuegos de aplicaciones web), el cual nos brinda una protección constante y un control mucho más eficiente y segregado permitiéndonos establecer reglas de prevención ante un posible ataque cibernético.

ABSTRACT

The purpose of this degree work is to implement a security mechanism or tool that allows analyzing, detecting, and filtering signs of cyber-attacks towards web applications that are developed internally in the company Seguros Alianza S.A. The importance of this purpose lies in the fact that cyber-attacks currently target various points within a technological infrastructure, such as the server where the web applications owned by the organizations with which the administration procedures and operations are carried out are hosted., productivity and business continuity, as well as the automation of internal processes.

In most cases there is no control or security policy for the development of secure web applications, since developers are unaware of a methodology that allows them to generate code that is secure or, in turn, due to time factors or deadlines that They are established in the projects, which must be complied with, so that developers focus more on the functionality of web applications than on their security.

A bad practice in the development of web applications as well as not giving the importance of the case to security would have consequences that could become extremely serious due to the sensitive data that users have, since personal data, bank details and other information that could be compromised by a computer criminal, generating a high risk for the organization.

In such a way that in the organizational environment it becomes essential to obtain or implement a mechanism that provides additional security for web applications and that the responsibility for security does not fall on the developer but rather that it is possible to have an intelligent and automated filter.

that allows detection of attacks on our web applications such as a WAF (Web

Application Firewall), which provides us with constant protection and much more efficient and segregated control, allowing us to establish prevention rules against a possible cyber-attack.

1. INTRODUCCIÓN

En el contexto actual, tanto a nivel nacional como mundial, la tecnología ha adquirido una importancia significativa, especialmente debido a la pandemia del COVID-19, que ha impactado en todos los aspectos de la sociedad. Las organizaciones se han visto obligadas a automatizar sus procesos para mejorar los tiempos de respuesta y adaptarse a la transformación digital. A lo largo de los años, la tecnología ha experimentado un crecimiento y evolución significativos, al igual que los ataques cibernéticos, que se han vuelto más efectivos a medida que los ciberdelincuentes perfeccionan sus técnicas para comprometer sistemas informáticos vulnerables con el objetivo de obtener beneficios económicos o robar información importante.

En Ecuador, al igual que en otros lugares del mundo, el sector asegurador ha experimentado el impacto de la era digital en los negocios. La implementación de sistemas de información, infraestructura tecnológica y la gestión de redes sociales han sido mecanismos clave para que las aseguradoras obtengan beneficios, como la captación de nuevos clientes, la fidelización de los existentes y la facilidad de gestión de pólizas de seguros. Seguros Alianza S.A., una empresa de seguros establecida en 1982, ha realizado mejoras continuas en todos los aspectos organizativos y considera la tecnología como uno de los pilares fundamentales de su lógica empresarial. Los sistemas de información brindan apoyo en la gestión laboral, facilitando los procesos diarios de los usuarios.

Sin embargo, a pesar de que los sistemas de información son desarrollados a medida para automatizar, facilitar o mejorar los procesos internos de una organización, siguen siendo vulnerables a ataques maliciosos. En el departamento de Tecnología de Seguros Alianza S.A. se ha llevado a cabo un análisis de la infraestructura tecnológica, y se ha determinado que las aplicaciones web utilizadas para la gestión y producción del negocio carecen de mecanismos de protección. La seguridad de las aplicaciones web es fundamental para proteger la información, prevenir el robo de datos, evitar

interrupciones en la continuidad del negocio y mitigar otras consecuencias perjudiciales derivadas de ataques cibernéticos.

Es común que muchas organizaciones no cuenten con los recursos económicos necesarios para implementar mecanismos de seguridad de la información, lo cual puede llevar a descuidar áreas críticas y perjudicar la continuidad del negocio. En el caso de Seguros Alianza S.A., la falta de protección adecuada crea una probabilidad latente de sufrir un ciberataque a corto, mediano o largo plazo, lo que podría resultar en la pérdida o alteración de información importante y comprometer los activos de la organización, causando pérdidas económicas y dañando su reputación.

En este contexto, la implementación de un Cortafuegos de aplicaciones web (WAF) es el mecanismo adecuado para proteger las aplicaciones web en la organización. Un WAF se encarga de proteger las aplicaciones web mediante filtros, monitorización y bloqueo del tráfico HTTP y HTTPS que se considera malicioso y que se dirige hacia dichas aplicaciones. Además, impide la salida de datos o información no autorizada. Su funcionamiento se basa en la implementación de políticas y reglas que permiten diferenciar entre el tráfico malicioso y el tráfico seguro.

La implementación de un WAF reducirá la probabilidad de sufrir un ataque cibernético en las aplicaciones web, proporcionando un control específico y monitoreo de las amenazas existentes. Esto brindará a Seguros Alianza S.A. la confiabilidad y seguridad necesarias para proteger su información confidencial. A diferencia de los dispositivos de seguridad tradicionales, como firewalls, IDS/IPS o antivirus, un WAF está diseñado específicamente para proteger las aplicaciones web contra ataques maliciosos.

Es importante destacar que la implementación de un WAF en Seguros Alianza S.A. no solo proporcionará una capa adicional de seguridad a las aplicaciones web, sino que también permitirá una detección proactiva de ataques a través de un filtro inteligente. Asimismo, se garantizará el rendimiento, la disponibilidad y la escalabilidad de la red, lo cual es fundamental para el manejo de transacciones en línea y la continuidad del negocio.

En Ecuador, se ha impulsado el incremento de la seguridad de la información, especialmente en el ámbito de las aplicaciones web, debido a su importancia para la continuidad de negocio de las organizaciones. En el caso de Seguros Alianza S.A., una empresa que maneja información sensible y confidencial resulta prioritario implementar una herramienta de seguridad que garantice la integridad y seguridad de su red. Actualmente, existen puntos de control y herramientas de protección en Seguros Alianza S.A., como el firewall lógico, pero se requiere una valoración previa para justificar y fortalecer estos puntos y garantizar la seguridad e integridad de la información.

2. DETERMINACIÓN DEL PROBLEMA

En los últimos años el uso de aplicaciones web ha ido creciendo significativamente dentro de las organizaciones puesto que la transformación digital ha sido el factor clave para que se implementen y automaticen nuevos procesos que permitan mejorar las operaciones, soportar la gestión del negocio y el contacto con los clientes, dando como resultado un mejor desempeño tecnológico para las organizaciones, pero así mismo resulta riesgoso exponer información sensible o delicada y mucho peor si no se cuenta con la protección adecuada donde lo más óptimo sería contar con la confiabilidad, integridad y disponibilidad de la información. Actualmente la implementación de mecanismos o herramientas que brinden y protejan la seguridad de las aplicaciones web implican costos elevados y la mayoría de las organizaciones no tienen los recursos necesarios para poderlos adquirir o simplemente tienen una protección básica lo cual no es suficiente para el actual ambiente tecnológico en el que nos desenvolvemos a diario donde constantemente se atacan y vulneran sistemas de información.

Sin embargo, existen organizaciones que tienen muy claro el enfoque y el panorama de la seguridad de la información y la ciberseguridad por lo cual buscan propuestas y soluciones eficaces que les permita reducir la probabilidad de sufrir un ataque cibernético dando como resultado la implementación de un WAF específicamente para brindar protección a las aplicaciones web que se utilizan dentro de la organización fortaleciendo la infraestructura tecnológica de la organización.

3.OBJETIVOS

Objetivo General

Realizar un análisis de la ciberseguridad en la infraestructura tecnológica de la empresa Seguros Alianza S.A., con un enfoque hacia la seguridad de las aplicaciones web para poder conocer la o las vulnerabilidades existentes mediante la implementación de un WAF, el cual es un mecanismo o solución tecnológica que brinda la seguridad necesaria al servidor de aplicaciones para que nos permita reducir los riesgos de ataques cibernéticos, mantener íntegra la seguridad de la información y que nos garantice la protección de los datos sensibles y confidenciales de la organización.

Objetivos Específicos

- Definir la línea base de ciberseguridad de la infraestructura tecnológica para identificar la capacidad, fortaleza y debilidad de la infraestructura actual de Seguros Alianza S.A.
- Crear el plan de remediación de vulnerabilidades identificadas de la arquitectura de red (infraestructura de conmutación, dispositivos de infraestructura, cumplimiento de políticas de red, etc.) de la organización.
- Ejecutar las fases del plan de remediación en un prototipo (infraestructura de conmutación, dispositivos de infraestructura, cumplimiento de políticas de red, etc.) para la mitigación de las principales vulnerabilidades según el nivel de criticidad.
- Evaluar los resultados obtenidos y generar las recomendaciones del proceso de evaluación conjunta para el robustecimiento de la arquitectura de ciberseguridad.

4. MARCO TEÓRICO REFERENCIAL

En las organizaciones se han analizado y desarrollado proyectos para poder llevar a cabo la implementación de un WAF, específicamente para brindar seguridad a las aplicaciones web, que mediante la configuración de filtros y reglas se establece un mecanismo de protección para prevención de ataques cibernéticos tomando medidas preventivas importantes y una correcta remediación, de esta manera se podrá tener el control y la monitorización del tráfico existente en la red.

En el presente capitulo se realizarán descripciones de los conceptos fundamentales para poder entender todo lo que engloba a la seguridad de aplicaciones web y la implementación de un WAF en una organización donde la lógica del negocio son los seguros.

4.1 Conceptos Generales

4.1.1 Ciberseguridad

La ciberseguridad o también denominada seguridad informática involucra la creación de políticas las cuales se las determina como un conjunto de procesos, controles y herramientas que apoyen a la protección de datos o la información confidencial, los sistemas o plataformas que son de ámbito comercial y otros activo tecnológicos. Adicionalmente también se la conoce como seguridad de las tecnologías de la información, es una práctica que cada vez se la considera más necesaria en un entorno cada vez más digitalizado y, por tanto, más vulnerable a sufrir ataques informáticos. [2]

Las políticas de ciberseguridad establecen las directrices y los lineamientos para proteger los activos digitales de la organización. Estas políticas definen los procesos y procedimientos para la gestión de riesgos, la prevención de amenazas, la

detección de intrusiones, la respuesta a incidentes y la recuperación ante desastres. Se basan en estándares y marcos de seguridad reconocidos, como ISO 27001, NIST Framework de ciberseguridad y CIS Controles, para garantizar una protección eficaz y adecuada.

La ciberseguridad se vuelve cada vez más crucial a medida que las organizaciones dependen cada vez más de la tecnología para sus operaciones comerciales. La protección de datos y sistemas se ha convertido en una prioridad estratégica, ya que las amenazas cibernéticas pueden resultar en pérdida de información confidencial, interrupción de servicios, daño a la reputación y pérdidas económicas significativas.

En conclusión, la ciberseguridad se ha convertido en una disciplina esencial para garantizar la protección y la resiliencia de las organizaciones en el entorno digital actual. Mediante la implementación de políticas sólidas, controles de seguridad efectivos y el uso de herramientas avanzadas, las organizaciones pueden mitigar los riesgos y proteger sus activos tecnológicos y su información confidencial de manera efectiva.

4.1.2 Seguridad de las aplicaciones web

La seguridad de las aplicaciones web menciona los diversos mecanismos, tecnologías y los diferentes métodos que son usados para realizar la protección de los servidores web, las aplicaciones web y los servicios web como lo son las API en contra de las amenazas que planifican los ciberataques de Internet. La seguridad de las aplicaciones web es primordial para que se pueda establecer la protección de los datos, los clientes y las organizaciones del robo de información, la interrupción del negocio u otras consecuencias devastadoras del ciberdelito. [3]

Además, la seguridad de las aplicaciones web implica la adopción de buenas prácticas en el desarrollo de software, como la programación segura, el uso de bibliotecas y marcos de trabajo actualizados, la realización de pruebas de seguridad y auditorías regulares, y la aplicación de parches y actualizaciones de seguridad.

También es importante mantenerse actualizado sobre las últimas amenazas y vulnerabilidades conocidas, como las mencionadas en el OWASP TOP 10, y aplicar las medidas de protección adecuadas para mitigar esos riesgos.

4.1.3 WAF

Un firewall de aplicaciones web (WAF) protege el servidor de aplicaciones web del lado del servidor contra muchos tipos de ataques. El trabajo de WAF es mantener seguros los servidores web mediante el análisis de patrones de tráfico y paquetes de solicitud HTTP y HTTPS. [4]

Los WAF también tienen la capacidad de realizar la protección y prevenir de los diferentes ataques que existen actualmente, lo cual un firewall de red u otras herramientas de prevención de intrusiones no lo pueden hacer. Un WAF se encuentra siempre por delante de la aplicación web por ende el tráfico de red debe pasar primero por esta herramienta realizando filtros antes de pasar a una aplicación web a su vez proporcionar un monitoreo de actividad de la aplicación generando alertas o bloqueando el tráfico que lo clasifica como malicioso o que a su vez no cumple con ciertas reglas de configuración.

El objetivo principal es detectar ataques a nivel de la capa de aplicación como inyecciones SQL, scripts maliciosos, intentos de manipulación de aplicaciones web, entre otros.

Un WAF trabaja mediante un modo llamado Reverse-Proxy, lo cual quiere decir que el tráfico de red procedente de los usuarios en internet que busca llegar a los servicios del cliente será bloqueado por el cortafuegos de aplicaciones web (WAF) el cual aplicará los respectivos controles y reglas de seguridad en capa de aplicación, para posteriormente enviar peticiones legítimas mediante nuevas sesiones hacia los diferentes servicios que se encuentren publicados. WAF es una plataforma o una herramienta de seguridad que se enfoca en la protección de aplicaciones web HTTP, HTTPS, FTP, FTPS y servicios web para enfrentar ataques en la capa 7 del modelo OSI la cual corresponde a la capa de aplicación, de esta

manera el tráfico es desviado exclusivamente a los protocolos que antes se los mencionó.

En la Figura 1 se mostrará una representación de las capas del modelo OSI, donde la capa número 7 es la que corresponde a la aplicación, dicha capa es la que muestra la información y los datos al usuario y con la que realiza la interacción.

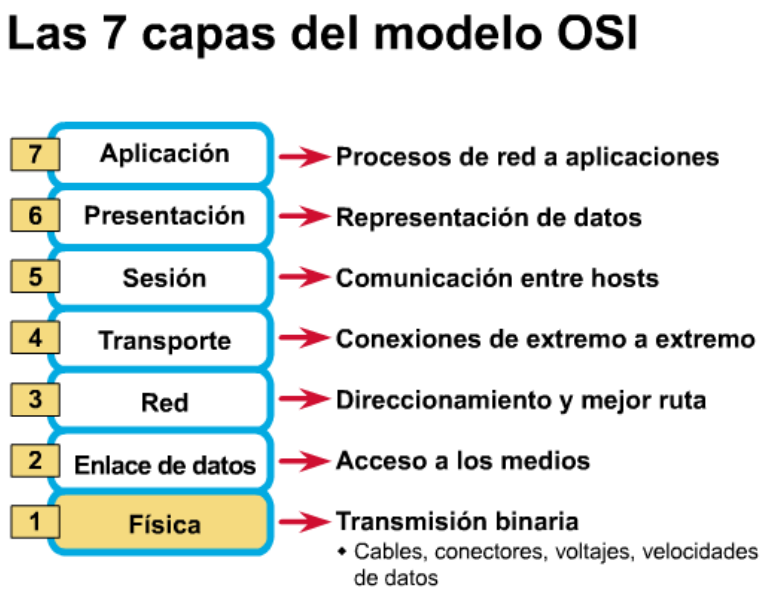


Figura 1. Representación de las capas del modelo OSI

Fuente: https://grd1503687jjfdog.blogspot.com/p/modelo-osi.html

4.1.4 Infraestructura tecnológica

El elemento básico de la organización es su infraestructura tecnológica. Se puede definir como un conjunto de elementos utilizados para almacenar datos comerciales dentro de una organización. Incluye tanto el hardware como el software y diversos servicios necesarios para optimizar la gestión interna y la seguridad de la información. [5]

La infraestructura tecnológica es un componente esencial para el funcionamiento de una organización, ya que proporciona el soporte necesario para almacenar, procesar y gestionar los datos comerciales de manera eficiente. Consiste en un

conjunto de elementos interrelacionados que incluyen hardware, software y servicios complementarios que permiten la operación y seguridad de la información.

En cuanto al hardware, la infraestructura tecnológica abarca servidores, equipos de almacenamiento, dispositivos de red, dispositivos móviles, sistemas de seguridad, entre otros. Estos componentes físicos son responsables de procesar y almacenar los datos necesarios para las operaciones comerciales de la organización.

Por otro lado, el software juega un papel fundamental en la infraestructura tecnológica, ya que incluye sistemas operativos, aplicaciones empresariales, herramientas de gestión y seguridad, bases de datos, entre otros. Estos programas informáticos permiten la ejecución de tareas específicas, el procesamiento de datos y la gestión de la información de manera eficiente y segura.

Además del hardware y el software, la infraestructura tecnológica requiere de diversos servicios para su optimización y seguridad. Estos servicios pueden incluir la gestión de redes, servicios de almacenamiento en la nube, servicios de respaldo y recuperación de datos, servicios de virtualización, servicios de seguridad informática, entre otros. Estos servicios complementarios garantizan un funcionamiento eficiente de la infraestructura y contribuyen a la protección de los datos comerciales contra posibles amenazas y pérdidas de información.

Es importante destacar que la infraestructura tecnológica debe ser diseñada y gestionada de manera adecuada para satisfacer las necesidades específicas de la organización. Esto implica la implementación de políticas de seguridad, configuraciones adecuadas, monitoreo constante y actualizaciones regulares para garantizar un entorno tecnológico seguro, confiable y eficiente.

4.1.5 Vulnerabilidades más habituales en la seguridad de las aplicaciones web

Los ataques contra aplicaciones web varían desde la manipulación de bases de datos atacadas hasta la interrupción de redes a gran escala.

- **Cross site scripting:** XSS es una vulnerabilidad que podría permitir a un atacante inyectar un script del lado del cliente en una página web para acceder a información confidencial, hacerse pasar por un usuario o engañar a un usuario para que revele información confidencial.
- **Inyección SQL**: es un método por el cual un atacante puede explotar una vulnerabilidad en la forma en que una base de datos ejecuta consultas de búsqueda. Los atacantes usan este método para acceder a información no autorizada, cambiar o crear nuevos derechos de usuario, o manipular o destruir datos confidenciales.
- **Ataques de denegación de servicio y ataques de denegación de servicio distribuido:** Usando diferentes vectores, un atacante puede sobrecargar un servidor dado o su infraestructura circundante con diferentes tipos de tráfico de ataque. Cuando un servidor ya no puede manejar las solicitudes entrantes de manera eficiente, comienza a ralentizarse y finalmente rechaza las solicitudes entrantes de usuarios legítimos.
- **Desbordamiento de búfer:** Un desbordamiento de búfer es una anomalía que ocurre cuando el software inserta datos en una ubicación de búfer específica en la memoria. Los desbordamientos de búfer pueden hacer que las ubicaciones de memoria adyacentes se sobrescriban con datos. Esta acción se puede usar para inyectar código malicioso en la memoria que puede causar vulnerabilidades en la máquina de destino.
- **Violación de los datos:** A diferencia de los vectores de ataque específicos, una violación de datos es un término general que se refiere a la exposición de información confidencial o sensible debido a una actividad maliciosa o un error.

Cualquier cosa, desde unos pocos registros valiosos hasta comprometer millones de cuentas de usuario, puede considerarse una violación de datos. [6]

4.1.6 Tipos de WAF

Si nos fijamos en cómo está configurado y en qué infraestructura está instalado, podemos clasificar los cortafuegos de aplicaciones web en tres tipos diferentes.:

- **WAF de red:** Se ubica físicamente en la red corporativa de la empresa concretamente, dentro de la DMZ o red perimetral, lo que maximiza la rapidez en el procesamiento de todas sus acciones.
- **WAF de host:** Vienen configuradas e instaladas directamente en el hosting. Se pueden implementar en el sistema operativo, en el servidor web o bien en la propia aplicación final.
- **WAF en la nube:** Los Cloud WAF no requieren de ninguna estructura ya que se implantan en la nube. Sirven para cualquier plataforma y se administran en remoto. [7]

4.1.7 Empresas aseguradoras

Las empresas de seguros, también conocidas como compañías aseguradoras, desempeñan un papel fundamental en la protección y garantía de los bienes y activos de terceros, brindando cobertura contra diversos riesgos a los que puedan estar expuestos. En el entorno actual, estas compañías han puesto un gran énfasis en la mejora continua de la atención al cliente y en ofrecer servicios de alta calidad.

Con la rápida evolución de las tecnologías de la información, como las aplicaciones web, las aplicaciones móviles, las telecomunicaciones y el internet, se ha generado una creciente competencia en el sector asegurador. La adopción de estas tecnologías ha permitido a las compañías de seguros obtener beneficios significativos, como la optimización de costos, la mejora en los tiempos de respuesta de las operaciones internas y, sobre todo, el aumento de la rentabilidad de sus operaciones, lo que se traduce en la satisfacción de sus clientes.

Las aplicaciones web y móviles han revolucionado la forma en que las compañías de seguros interactúan con sus clientes, ofreciendo servicios más accesibles, personalizados y eficientes. Estas aplicaciones permiten a los clientes realizar transacciones en línea, como solicitar cotizaciones, gestionar pólizas, presentar reclamaciones y recibir asesoramiento especializado, todo ello desde la comodidad de sus dispositivos móviles o computadoras.

Además, las tecnologías de telecomunicaciones e internet han facilitado la comunicación y colaboración interna en las empresas de seguros, permitiendo una mayor agilidad en los procesos y una optimización de los recursos. La implementación de sistemas de gestión integrados, el uso de plataformas de colaboración y el aprovechamiento de herramientas de análisis de datos han contribuido a una mejor toma de decisiones y a una mayor eficiencia en la gestión de los riesgos y los reclamos.

4.1.8 Solución WAF de FortiWeb

FortiWeb WAF (cortafuegos de aplicaciones web) es una solución avanzada que ofrece una amplia gama de funciones para proteger aplicaciones web y APIS contra amenazas tanto conocidas como de día cero. Con su enfoque multicapa y sofisticado, FortiWeb se encarga de proteger contra las 10 principales amenazas identificadas por OWASP, así como otras amenazas adicionales.

Una de las características destacadas de FortiWeb es su capacidad de adaptar la protección a cada aplicación específica. Utilizando técnicas de aprendizaje automático, FortiWeb puede ajustar su protección de forma inteligente sin requerir configuraciones manuales laboriosas que suelen ser necesarias en otras soluciones. Mediante el uso del aprendizaje automático, FortiWeb es capaz de identificar comportamientos anómalos en las aplicaciones web y, lo que es aún más importante, distinguir entre anomalías maliciosas y benignas.

Además de la protección contra amenazas, FortiWeb incluye también una mitigación efectiva de robots web. Esta funcionalidad permite permitir el acceso de

robots web benignos, como los motores de búsqueda, mientras bloquea de manera consistente los robots web maliciosos que intentan comprometer la seguridad de las aplicaciones. Esto garantiza que los robots web legítimos puedan acceder e indexar el contenido adecuadamente, mientras se mantienen a raya los robots web maliciosos que pueden tener intenciones nefastas.

FortiWeb ofrece opciones de implementación que pueden proteger las aplicaciones comerciales sin importar dónde estén alojadas. Las capacidades incluyen dispositivos dedicados, máquinas virtuales y contenedores que se pueden implementar en centros de datos, entornos de nube o dentro de la solución SaaS nativa de la nube de FortiWeb Cloud, WAF como servicio. [8]

4.1.9 OWASP

OWASP (Proyecto abierto de seguridad de aplicaciones web) es una fundación sin fines de lucro con sede en Estados Unidos que se dedica a promover la seguridad en aplicaciones web a través de proyectos de código abierto. Su objetivo principal es identificar y definir las vulnerabilidades comunes en el software inseguro y proporcionar metodologías, documentación y herramientas para abordar estos problemas de seguridad.

La fundación trabaja de manera continua para desarrollar y difundir recursos que están disponibles de forma gratuita. Uno de los documentos más importantes y reconocidos a nivel mundial es el OWASP Top 10. Este informe se actualiza cada tres años y proporciona un análisis exhaustivo de los riesgos de seguridad en las aplicaciones web.

El OWASP Top 10 es una lista de los diez riesgos más comunes que enfrentan las aplicaciones web en términos de seguridad. Es de vital importancia comprender el conjunto de vulnerabilidades que se incluyen en esta lista, ya que proporciona una guía invaluable para el análisis de riesgos y la implementación de medidas de seguridad en aplicaciones web.

Al comprender los riesgos y vulnerabilidades presentados en el OWASP Top 10, las organizaciones pueden tomar medidas proactivas para mitigar y prevenir estos riesgos en sus aplicaciones. Esto implica la implementación de herramientas y controles de seguridad adecuados para proteger las aplicaciones web contra amenazas comunes, como inyección de código, autenticación y autorización defectuosas, exposición de datos sensibles, entre otros.

4.1.10 OWASP TOP 10 Actualización y Comparación entre 2017 y 2021

Al analizar las actualizaciones en el informe OWASP Top 10, se pueden identificar las tendencias emergentes en los ataques cibernéticos dirigidos a aplicaciones web. Estas tendencias incluyen nuevas técnicas de explotación, cambios en las prioridades de seguridad y enfoques de mitigación actualizados.

Esta sección es fundamental para entender el contexto de la protección de las aplicaciones web dentro de una organización, ya que OWASP detalla información que se debe tener en consideración para la implementación y el desarrollo de software seguro y en la configuración de herramientas de seguridad como lo es un WAF.

La comparación entre las versiones de 2017 y 2021 del informe OWASP Top 10 es esencial para comprender la evolución de las amenazas y los enfoques de seguridad en el ámbito de las aplicaciones web. Esto permite a las organizaciones mantenerse actualizadas sobre las nuevas vulnerabilidades y adaptar sus estrategias de protección en consecuencia.

La Figura 2 muestra los cambios en base a las tácticas que son utilizadas por los ciberdelincuentes para vulnerar las aplicaciones web que se encuentren implementadas en los diferentes segmentos corporativos, dichos cambios se

dan según la clasificación que fue creada en el año 2017 y posteriormente fue actualizada en el año 2021.

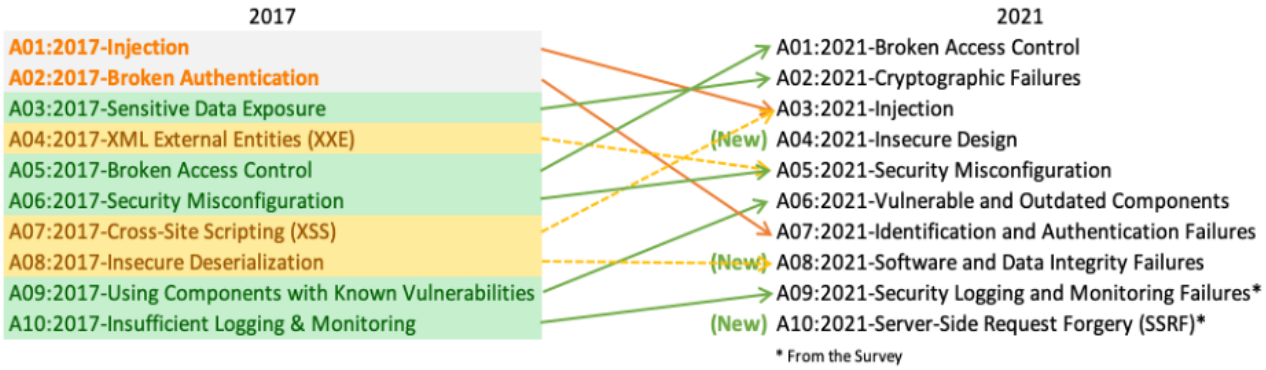


Figura 2. Comparativa de OWASP Top 10 entre el año 2017 y 2021

Fuente: https://owasp.org/www-project-top-ten/

A continuación, se detallan los cambios:

- **A01: 2021 - Fallos de control de acceso**, En un detalle anterior de las 10 principales vulnerabilidades de aplicaciones web de 2017, el riesgo ocupó el quinto lugar. Sin embargo, un estudio reciente de OWASP probó el riesgo en el 94 % de las aplicaciones de análisis y mostró una incidencia del 3,81 %.

  Esta categoría se refiere a las vulnerabilidades encontradas al hacer cumplir los controles de autenticación y autorización. En otras palabras, el papel del control de acceso en las aplicaciones web es evitar que los usuarios hagan cosas que no pueden hacer.

  Al programar recursos web, los desarrolladores deben considerar esquemas de control de acceso y sistemas de permisos. En este sentido, se debe implementar un mecanismo de autenticación al acceder a cada recurso. Esto asegura que el usuario tenga asignados los roles necesarios para realizar acciones relacionadas con ese recurso.

- **A02: 2021 - Fallos criptográficos**, Este tipo de riesgo subió un lugar entre las 10 principales vulnerabilidades de aplicaciones web de 2017. Los errores relacionados con la criptografía entran en esta categoría. También puede filtrar datos confidenciales y comprometer todo el sistema.

Por lo tanto, la vulnerabilidad está relacionada con la falta de un protocolo de comunicación seguro y el problema utiliza:

- Esquemas de cifrado obsoletos y/o inseguros.
- Claves de cifrado débiles.

- **A03: 2021 - Inyección**, Esta categoría ha descendido del 1.er al 3.er lugar en la lista de las 10 principales vulnerabilidades de aplicaciones web, pero sigue siendo una vulnerabilidad crítica con una prevalencia del 3,37 %.

  Las vulnerabilidades de inyección permiten a un atacante cambiar el código funcional de una aplicación aprovechando la falta de filtrado o desinfección adecuados de los datos de entrada.

  Así es como se realizan acciones o se devuelve información de forma inesperada. Estos tipos de vulnerabilidades a menudo tienen un impacto significativo en la seguridad de las aplicaciones web.

- **A04: 2021 - Diseño inseguro**, Esta categoría es de nueva creación e incluye varios riesgos relacionados con el diseño web y errores de arquitectura. O agrupar de manera similar un conjunto de debilidades que resultan de no aplicar un enfoque de diseño seguro.

  Estas vulnerabilidades son difíciles de parchear una vez desarrolladas. Esto se debe tanto a la complejidad de la tarea como al costo adicional de realizarla. En ese sentido, OWASP marca una diferencia que vale la pena tener en cuenta. No es lo mismo un diseño inseguro que una implementación insegura. Los errores de implementación que crean vulnerabilidades pueden dificultar los diseños seguros.

  Los inconvenientes de un diseño inseguro no se pueden mitigar con una implementación libre de errores. Porque no hay controles de seguridad para protegerse contra ciertos ataques. Un factor importante en el diseño inseguro

es la incapacidad de una organización para determinar qué nivel de diseño seguro se requiere.

- **A05: 2021 - Configuración errónea de seguridad**, La arquitectura de una aplicación web se basa en una serie de elementos que ofrecen diferentes opciones de configuración. Servidores, marcos de trabajo, sistemas de gestión de datos, CMS, plugin, APIS, todos estos elementos pueden formar parte de la arquitectura que soporta tu aplicación. Puede ocurrir una brecha de seguridad si la configuración es incorrecta o si la configuración predeterminada no cumple con buenos estándares de seguridad.

  Este error se encontró en cuatro aplicaciones web probadas en la encuesta OWASP. Esto lo convirtió en la lista de las 10 principales vulnerabilidades de aplicaciones web para 2017.

- **A06: 2021 - Componentes vulnerables y obsoletos**, Estos tipos de vulnerabilidades son causadas por el uso de software o componentes obsoletos o vulnerabilidades conocidas en su aplicación o infraestructura web.

  ¿Cómo saben las empresas cuándo sus aplicaciones web están en riesgo debido a componentes vulnerables o desactualizados? OWASP enumera seis situaciones en las que las organizaciones pueden revelar este problema: Estoy especificando.

  - No se conocen las versiones de todos los componentes que se están utilizando en la aplicación web. Tanto del lado del cliente, como del lado del servidor.
  - El software es vulnerable, no tiene soporte o está desactualizado.
  - No se escanean las vulnerabilidades regularmente.
  - No se corrige o actualiza la plataforma subyacente y los marcos de trabajo.
  - Los desarrolladores de software no comprueban la compatibilidad entre las bibliotecas actualizadas o parcheadas.

- No se garantiza la seguridad de las configuraciones de todos los componentes.

- **A07: 2021 - Fallos de identificación y autenticación**, Esta categoría se denomina Fallo de autenticación en las 10 principales vulnerabilidades de aplicaciones web de 2017. 2do lugar en este ranking. Esta vez, el equipo de OWASP decidió agrupar fallas de autenticación e identificación y encontró tales vulnerabilidades en 2.55 de las aplicaciones probadas.
- **A08: 2021- Fallos de integridad de datos y software**, Estos tipos de errores están relacionados con la falta de protección del código y de la infraestructura frente a violaciones de la integridad. Esta categoría es una nueva categoría en las 10 principales vulnerabilidades de aplicaciones web. Se utiliza para centrarse en las debilidades relacionadas con:

  - Ataques maliciosos a las cadenas de suministro de software.
  - Plugin, bibliotecas, repositorios y redes de entrega de contenido no fiables.
  - Canales CI/CD inseguros, a través de los que se puede introducir códigos maliciosos o comprometer el sistema.
  - Funcionalidades de autoactualización en las que las actualizaciones se descargan sin contar previamente con un sistema seguro de verificación de la integridad. A través de esta vía de acceso, los ciberdelincuentes pueden subir sus propias actualizaciones maliciosas para distribuirlas y ejecutarlas en todas las instalaciones.

- **A09: 2021 - Fallas de registro y monitoreo de seguridad**, En primer lugar, la trazabilidad de los eventos que ocurren en su aplicación es esencial para frustrar las amenazas. Luego, examine los incidentes de seguridad que ya han ocurrido para evitar que se repitan e identificar los activos que puedan estar en riesgo.

  Esta categoría está diseñada para ayudar a los profesionales a detectar, escalar y responder a las infracciones de seguridad activas. Es posible que no pueda

detectar, detectar, monitorear y responder proactivamente a los ataques en las siguientes situaciones:

- Los eventos auditables, como los inicios de sesión o las transacciones de alto valor no se registran.
- Las advertencias y los errores no generan mensajes de registro o son inadecuados.
- Los registros de las aplicaciones y las API no se supervisan.
- Los registros solo se almacenan localmente.
- Las pruebas de penetración no activan las alertas de seguridad.
- La aplicación web es incapaz de detectar, escalar y alertar ataques en tiempo real.

- **A10: 2021 - La falsificación de solicitudes del lado del servidor**, Este tipo de vulnerabilidad ocurre cuando un atacante puede obligar a un servidor a conectarse a un objetivo no deseado. De esta forma, los atacantes pueden aprovechar la posición privilegiada del servidor dentro de la infraestructura para:

  - Evadir cortafuegos.
  - Forzar conexiones a elementos de la red interna.
  - Interactuar con recursos que inicialmente eran restringidos.
  - Esta última categoría del Top 10 de vulnerabilidades en aplicaciones web es de nueva creación y no responde tanto a los datos obtenidos tras testear aplicaciones, sino a los resultados de la encuesta realizada por OWASP a expertos en ciberseguridad de todo el mundo. [9]

4.2 Métodos de Recolección de Información

Para llevar a cabo este análisis de manera rigurosa, se empleará una combinación de métodos de recopilación y revisión de documentos, análisis detallado de

registros de eventos y la recolección de información valiosa a través de entrevistas con el personal del departamento de Tecnología, especialmente del Área de Operaciones. Estas actividades permitirán obtener una visión integral de los requisitos técnicos necesarios para la implementación exitosa del WAF y, al mismo tiempo, proporcionarán información relevante sobre el historial de implementaciones de seguridad en la infraestructura tecnológica de la organización, lo que permitirá conocer el estado actual de la red y las posibles vulnerabilidades existentes.

Asimismo, se llevarán a cabo entrevistas exhaustivas con el equipo de operaciones y los usuarios funcionales que posean conocimiento especializado sobre las aplicaciones web de la organización. Estas entrevistas se realizarán con el objetivo de obtener información complementaria que contribuya a una identificación más precisa y detallada de las necesidades específicas de la organización en cuanto a la seguridad de las aplicaciones web. El conocimiento y la experiencia de estos profesionales serán fundamentales para comprender a fondo los desafíos y las amenazas potenciales que enfrenta Seguros Alianza S.A.

Con el fin de implementar de manera efectiva el WAF y obtener la información necesaria para garantizar su correcto funcionamiento, se programarán reuniones periódicas con el equipo de SKYTECHNOSA, quienes son expertos en soluciones de seguridad informática. Durante estas reuniones, se realizarán configuraciones específicas y se establecerán reglas adecuadas en el WAF, todo ello basado en las aplicaciones web y los requerimientos específicos de Seguros Alianza S.A. Este enfoque personalizado permitirá adaptar las soluciones de seguridad a las necesidades específicas de la organización y garantizar la eficacia del WAF en la protección contra amenazas cibernéticas.

Además, se llevarán a cabo pruebas rigurosas en colaboración con el equipo de desarrollo, interactuando directamente con las diversas aplicaciones web que se encuentran en producción dentro de la organización. Estas pruebas, tanto de funcionalidad como de seguridad, serán fundamentales para verificar la efectividad

del WAF en un entorno real y asegurar que cumpla con los estándares más altos de protección. Las pruebas también ayudarán a identificar posibles brechas de seguridad y a realizar ajustes o mejoras necesarios antes de la implementación final.

Con el fin de respaldar y documentar todo el proceso de implementación y pruebas, se recopilarán minuciosamente las evidencias de las reuniones mantenidas con el personal de SKYTECHNOSA. Estas evidencias incluirán detalles técnicos, informes de pruebas, registros de configuración y cualquier otra información relevante que respalde las decisiones tomadas durante el proceso de implementación.

En conclusión, este estudio se basa en un análisis detallado y exhaustivo de las soluciones de un WAF para la infraestructura tecnológica de Seguros Alianza S.A., empleando una metodología rigurosa de recopilación de información, entrevistas especializadas y pruebas colaborativas. El objetivo final es garantizar la selección e implementación adecuada de un WAF que cumpla con los más altos estándares de seguridad y protección, asegurando así la integridad y la confidencialidad de las aplicaciones web y los activos de información de la organización.

A continuación, se presentan las evidencias de las reuniones que se mantuvieron con el personal de SKYTECHNOSA en donde se realizaban pruebas, configuraciones e implementación del WAF en base a las aplicaciones web y requerimientos de Seguros Alianza S.A.

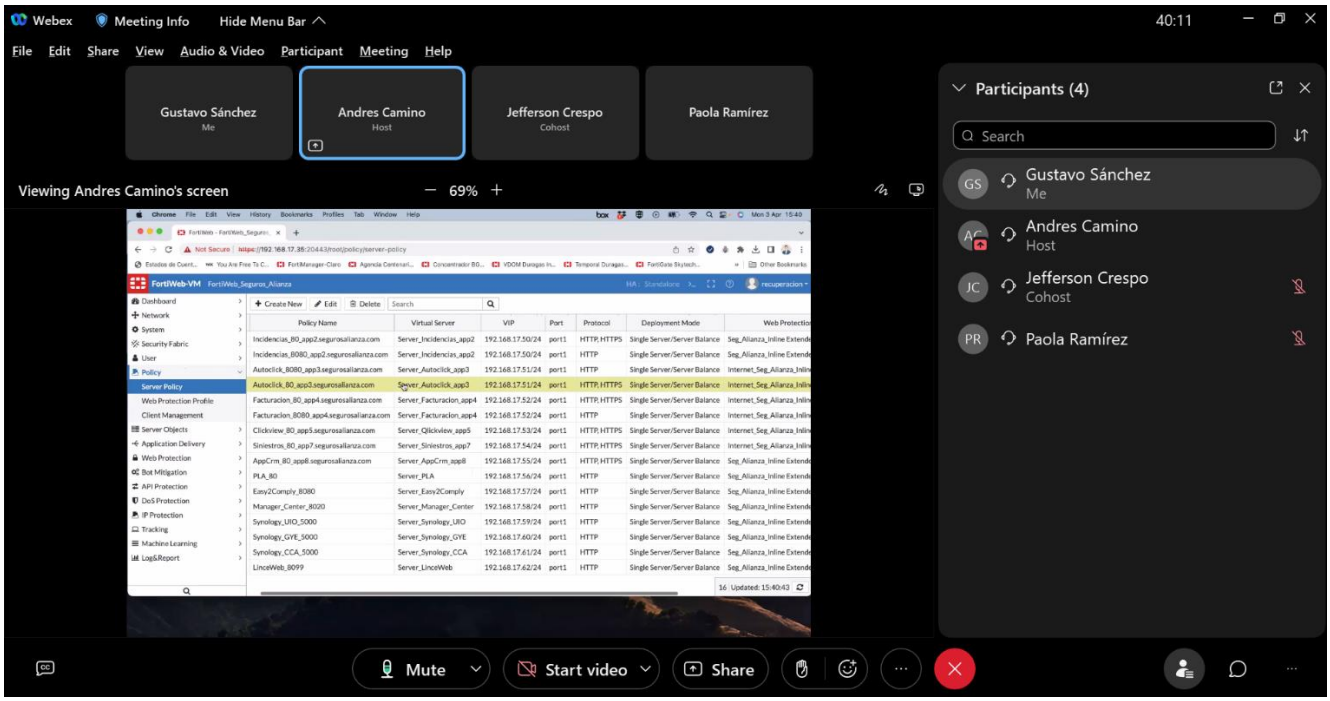


Figura 3. Políticas de servidor y asignación de IP virtuales

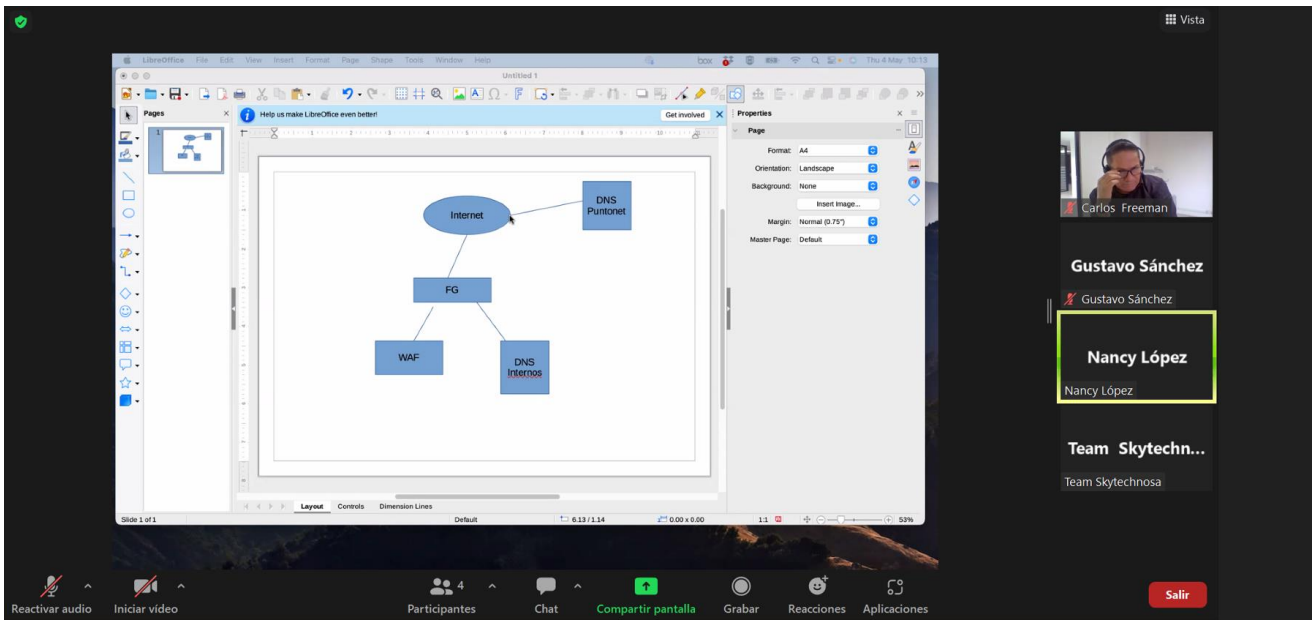


Figura 4. Análisis de infraestructura tecnológica de Seguros Alianza S.A.

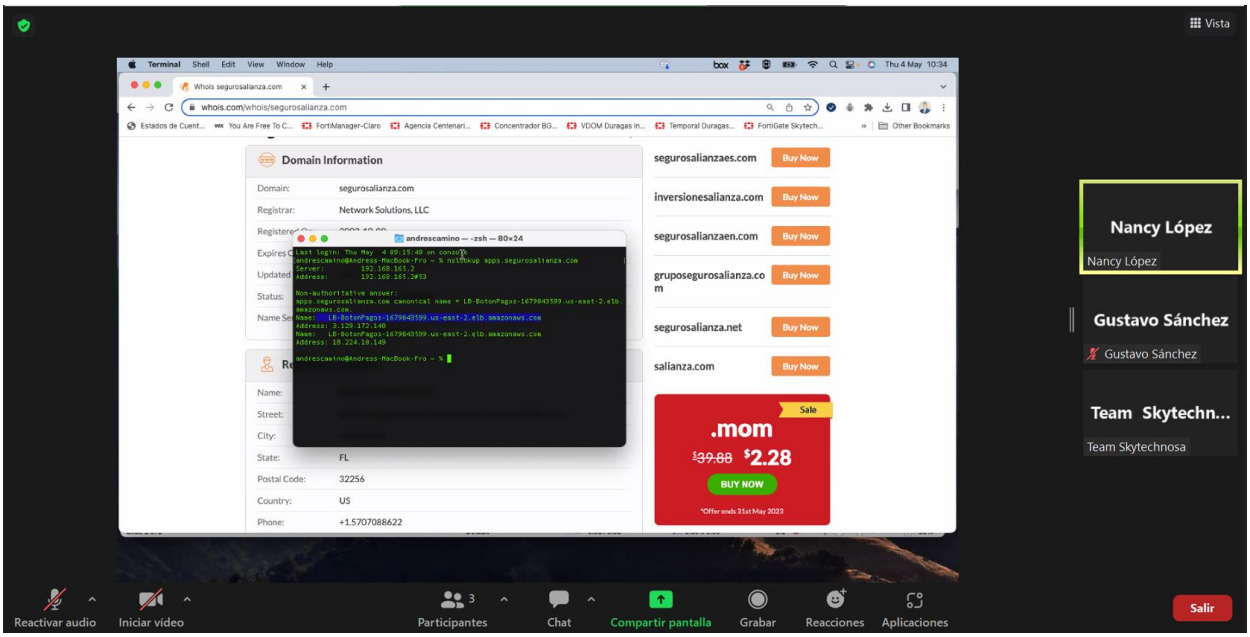


Figura 5. Verificación de nombre del dominio de Seguros Alianza S.A.

4.2.1 Obtención de Información

En la presente investigación se emplearán diferentes orígenes de información para recopilar los datos necesarios y obtener un panorama completo del tema en estudio.

En primer lugar, se utilizará el origen primario de información, el cual consiste en obtener los datos a partir de archivos digitales, reportes estadísticos, informes de riesgos e históricos actuales. Estos documentos proporcionarán información detallada sobre el estado actual de la organización y su infraestructura tecnológica. Además, se podrán analizar los datos específicos que describan el contexto en el que se desenvuelve la entidad, permitiendo identificar posibles vulnerabilidades y áreas de mejora.

En segundo lugar, se utilizará el origen secundario de información, el cual se basa en adquirir datos de diferentes páginas web especializadas en el tema de estudio,

así como de artículos científicos, académicos y documentos almacenados en repositorios web. Estas fuentes de información en internet proporcionarán una visión más amplia y actualizada del campo de estudio, permitiendo acceder a investigaciones previas, estadísticas relevantes y mejores prácticas en el ámbito de la seguridad cibernética y la protección de aplicaciones web.

Por último, se empleará el origen terciario de información, el cual consiste en adquirir conocimientos a través de manuales, tutoriales virtuales y recursos multimedia. Estas fuentes de información serán de gran utilidad para comprender conceptos técnicos, metodologías de seguridad, y herramientas específicas relacionadas con la protección de aplicaciones web. Se buscará obtener información necesaria y requerida, de manera clara y didáctica, que facilite el análisis y la comprensión de los aspectos relevantes en el desarrollo de la investigación.

La combinación de estos diferentes orígenes de información permitirá obtener un enfoque integral y sólido para abordar el tema de estudio. Además, garantizará que la investigación se base en datos confiables, actualizados y respaldados por expertos en el campo de la seguridad cibernética y las aplicaciones web.

4.3 Línea Base De Ciberseguridad De La Infraestructura Tecnológica

Dentro de la arquitectura tecnológica, se ha implementado un firewall de Fortinet como mecanismo de seguridad. Este firewall se encarga de proteger la red contra el tráfico no deseado mediante un conjunto de reglas previamente establecidas y programadas, bloqueando así la entrada de programas malignos y otras amenazas cibernéticas. El firewall de Fortinet actúa como una barrera de seguridad que filtra y controla el flujo de datos entre la red interna y externa, asegurando que solo los datos seguros y autorizados pasen a través de la red.

Adicionalmente, se han establecido reglas en el firewall para bloquear sitios web y aplicaciones específicas. Esto tiene como objetivo evitar que los usuarios accedan a páginas web prohibidas o realicen instalaciones de programas no autorizados dentro de la organización. Estas reglas de filtrado de contenido proporcionan una capa adicional de seguridad y ayudan a prevenir la exposición a amenazas potenciales que pueden estar asociadas con el acceso a sitios web no confiables o la descarga de software malicioso.

Como medida adicional de seguridad, se utiliza el servidor de antivirus ESET. Este servidor de antivirus está diseñado para prevenir y detectar anomalías en los equipos de la organización, identificando y eliminando cualquier software malicioso que pueda comprometer la seguridad de los sistemas. Además, se han establecido reglas específicas en el servidor de antivirus para evitar la infección de virus y bloquear a usuarios no autorizados, reduciendo así el riesgo de intrusiones no deseadas y protegiendo los activos digitales de la organización.

Por último, pero no menos importante, se encuentra la seguridad del directorio activo. El directorio activo es una parte fundamental de la infraestructura tecnológica de Seguros Alianza S.A., ya que es el servicio de directorio que gestiona y controla el acceso a los recursos de red. Mediante la implementación de políticas de seguridad sólidas en el directorio activo, se asegura que solo los usuarios autorizados tengan acceso a los sistemas y recursos de la organización. Esto implica la asignación adecuada de permisos y privilegios, la implementación de políticas de contraseñas robustas y la supervisión activa de los registros de eventos para detectar posibles actividades sospechosas.

A pesar de las medidas de seguridad implementadas, es importante destacar que la infraestructura tecnológica de Seguros Alianza S.A. presenta varias vulnerabilidades y un alto riesgo de sufrir ataques, especialmente en lo que respecta a la protección de las aplicaciones web. Las aplicaciones web suelen ser un objetivo frecuente de los ciberdelincuentes, ya que pueden presentar vulnerabilidades que podrían ser

explotadas para acceder a datos sensibles o comprometer la integridad de los sistemas.

Para mitigar estos riesgos, es recomendable que Seguros Alianza S.A. adopte medidas adicionales de seguridad. Esto puede incluir la implementación de firewalls de aplicaciones web, que se centran específicamente en proteger las aplicaciones y sus vulnerabilidades.

Estos firewalls analizan y filtran el tráfico web, identificando y bloqueando cualquier actividad sospechosa o maliciosa. Asimismo, se sugiere realizar pruebas de penetración regulares en las aplicaciones web para identificar vulnerabilidades y corregirlas antes de que sean aprovechadas por los atacantes.

Además de las medidas técnicas, es esencial mantenerse actualizado con las mejores prácticas de seguridad y capacitar al personal en ciberseguridad. La concientización y la educación en seguridad cibernética son fundamentales para garantizar que todos los empleados comprendan los riesgos y las mejores prácticas de seguridad, como el uso de contraseñas seguras, la protección de información confidencial y la identificación de posibles amenazas.

Con base en la evaluación realizada de la totalidad de la infraestructura tecnológica de Seguros Alianza S.A., se procederá a clasificar la información en distintos aspectos con el fin de identificar las fortalezas y debilidades inherentes a la estructura tecnológica de la organización:

ANÁLISIS DE SEGURIDAD

- **Firewalls y Seguridad de Red**
  - La configuración y efectividad del firewall se encuentra correctamente establecida.
  - Las políticas de seguridad de red se encuentran desactualizadas.

- **Antivirus y Antimalware**
  - El software de seguridad existente se encuentra correctamente actualizado.
  - El software de seguridad existente se encuentra realizando escaneos periódicos de virus y programas malignos.
- **Actualizaciones y Parches**
  - Existen servidores que no cuentan con una oportuna acción de instalación de actualizaciones.

RESPALDO Y RECUPERACIÓN

- **Copia de Seguridad de Datos**
  - Las políticas de respaldo y recuperación robustas se encuentran correctamente establecidas y se las está llevando a cabo.
  - Si se realizan pruebas periódicas de restauración.
- **Planes de Continuidad del Negocio**
  - Existe un plan para la continuidad del negocio en caso de fallos, pero se encuentra desactualizado.

GESTIÓN DE ACTIVOS Y CONFIGURACIÓN

- **Inventario de activos**
  - Si se lleva a cabo un inventario actualizado de todos los activos de hardware y software, este inventario se lo hace constantemente puesto que existe personal en la organización que deja sus funciones
- **Gestión de Configuración**
  - No se tiene implementado un sistema de gestión de configuración para controlar los cambios.

CAPACITACIÓN Y CONCIENCIACIÓN

- **Programas de Concienciación**
  - Existen programas de concienciación en seguridad para el personal
- **Capacitación Técnica**
  - Se brindan capacitaciones técnicas y continuas para el personal de TI

ACTUALIZACIÓN TECNOLÓGICA

- **Evaluación de Tecnologías Emergentes**
  - El personal de TI permanece informado constantemente mediante boletines y charlas de las nuevas tecnologías existentes o que se encuentran próximamente a salir al mercado y evalúa su aplicabilidad
- **Ciclo de Vida de los Equipos**
  - Cada determinado tiempo el personal encargado de TI evalúa y planifica la sustitución de equipos obsoletos, de esta manera se dan de baja los equipos mediante la gestión con RRHH

REVISIÓN Y MEJORA CONTINUA

- **Revisiones Periódicas**
  - Se realiza revisiones periódicas de la infraestructura con el personal de TI y personal externo y se realizan los respectivos ajustes según sea necesario
- **Retroalimentación del Usuario**
  - Existe una persona encargada del departamento de TI que recopila retroalimentación del usuario de todos los departamentos para identificar posibles áreas de mejora

Con la clasificación detallada se ha podido identificar de manera precisa los activos, comprender su capacidad y potencial, así como las fortalezas y debilidades proporcionando una base sólida para la toma de decisiones estratégicas. En este proceso se pudo abordar las debilidades y adaptación al cambio que continuamente y a medida evoluciona la tecnología. Se maximizó el rendimiento actual sentando las bases para una adaptación futura, promoviendo la innovación y la eficiencia en un entorno tecnológico dinámico.

4.3.1 Topología

A continuación, se muestra un esquema de la estructura de red de Seguros Alianza S.A. matriz, la cual es una representación de manera visual de la interacción y comunicación entre los diversos componentes que la conforman. Este gráfico exhibe los dispositivos, conexiones y rutas que se utilizan en la red para facilitar la comprensión de su funcionamiento en conjunto.

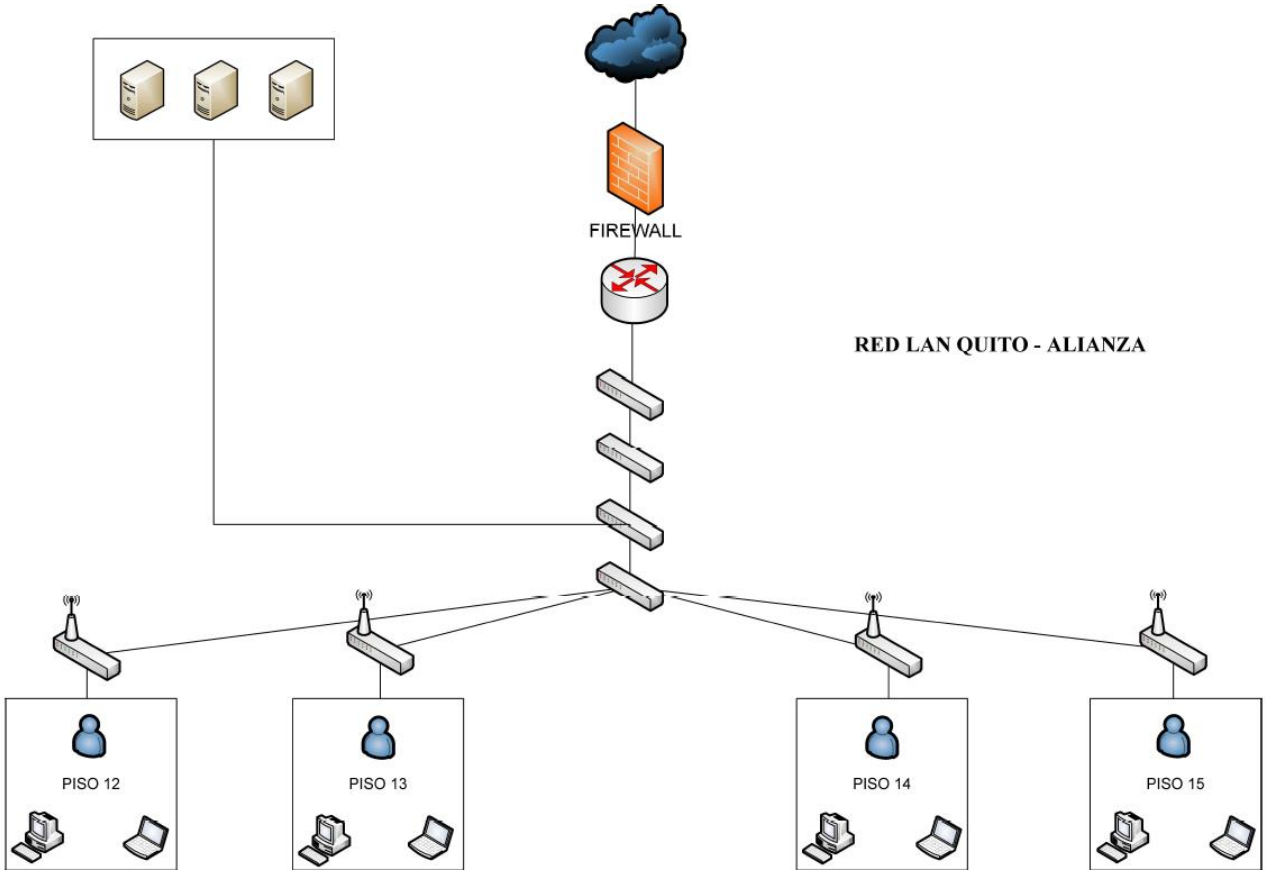


Figura 6. Topología de Red de Seguros Alianza S.A. Matriz

Fuente: Seguros Alianza S.A.

4.3.2 Evaluación de Activos

En el contexto de nuestra investigación sobre la infraestructura tecnológica de Seguros Alianza S.A. y su línea base de ciberseguridad, es fundamental llevar a cabo una evaluación exhaustiva de los activos de información críticos de la organización. Esta evaluación nos permitirá identificar y clasificar los diferentes activos, comprendiendo su importancia y valor dentro del entorno empresarial.

Para comenzar, es necesario identificar los activos de información críticos que forman parte de la infraestructura tecnológica de Seguros Alianza S.A. Un enfoque sistemático y detallado nos permitirá tener una visión clara de todos los activos relevantes y asegurarnos de que ninguno se escape de nuestra evaluación.

Una vez identificados los activos, es importante clasificarlos en función de su valor para la organización. Al asignar un valor a cada activo, podemos establecer una jerarquía de importancia y priorizar los recursos de seguridad en consecuencia. Por ejemplo, un sistema central que almacena información crítica de los clientes puede considerarse un activo de alto valor, mientras que una base de datos de respaldo puede ser menos crítica en términos de su impacto en las operaciones del negocio.

Es importante destacar que el valor de un activo no solo se basa en su importancia para la organización, sino también en el riesgo asociado a su compromiso. Por ejemplo, los datos personales de los clientes pueden tener un alto valor debido a su sensibilidad y al riesgo potencial de violación de la privacidad. Por lo tanto, la clasificación de los activos debe considerar tanto su importancia para la organización como el riesgo de exposición a amenazas y ataques.

Al comprender y clasificar los activos de información críticos, Seguros Alianza S.A. estará en una mejor posición para asignar recursos adecuados de seguridad y proteger eficazmente sus activos más valiosos. Esto implica implementar medidas de seguridad adecuadas, como controles de acceso, cifrado de datos, monitoreo de

seguridad y sistemas de respaldo, en función de la importancia y el riesgo asociado a cada activo.

NRO. ACTIVO	ACTIVO DE INFORMACIÓN	CANTIDAD	DESCRIPCIÓN	TIPO	PROCESOS RELACIONADOS	CRITICIDAD
A1	Servidor	1	Aplicaciones web de incidencias, inventarios, procesos y ajustes contables	Equipo Informático	Operaciones-Soporte TI, RRHH, Contabilidad	Alto
A2	Servidor	1	Aplicación web para la gestión y emisión de pólizas	Equipo Informático	Comercial, Administrativo	Alto
A3	Servidor	1	Aplicación web de facturación electrónica (facturas, notas de crédito, retenciones y liquidaciones de compras)	Equipo Informático	Proyectos, Tesorería, Contabilidad	Alto
A4	Servidor	1	Aplicación web para el control de riesgos	Equipo Informático	Riesgos, Operaciones-Soporte TI	Bajo
A5	Servidor	1	Sistema de gestión, administración y emisión de pólizas IBM-AS400	Equipo Informático	Operaciones-Soporte TI, Proyectos	Alto
A6	Servidor	1	Aplicación web de PLA (Prevención de lavado de activos)	Equipo Informático	Cumplimiento, Operaciones-Soporte TI, Proyectos	Bajo
A7	Servidor	1	Directorio Activo	Equipo Informático	Operaciones-Soporte TI	Alto

A8	Servidor	1	Aplicación web de Inspecciones de vehículos	Equipo Informático	Comercial, Siniestros, Proyectos	Medio
A9	Servidor	1	Aplicación web de Oficina Virtual (siniestros, clientes, corredores y colaboradores)	Equipo Informático	Comercial, Siniestros, Proyectos, Procesos	Alto
A10	Firewall de Fortigate	1	Gestión de autorización y restricciones de seguridad en el perímetro de la red de la organización	Software	Operaciones-Soporte TI	Alto
A11	Switch	4	Comunicación entre los dispositivos conectados y gestión del tráfico de datos internos	Redes de Comunicación	Operaciones-Soporte TI	Medio
A12	Router	6	Enrutamiento y la gestión del tráfico de datos permitiendo la comunicación de redes y dispositivos conectados	Redes de Comunicación	Operaciones-Soporte TI	Medio
A13	Wireless	5	Dispositivos de conexión inalámbrica distribuidos por toda la organización	Redes de Comunicación	Operaciones-Soporte TI	Alto
A14	Equipos de Escritorio	73	Estación de trabajo personal	Equipo Informático	Todos los procesos de la organización	Bajo

A15	Laptops	35	Estación de trabajo personal portátil	Equipo Informático	Todos los procesos de la organización	Bajo
A16	Bases de Datos	1	Bases de datos IMB DB2	Servicio	Operaciones-Soporte TI, Proyectos	Alto
A17	Intranet	1	Información interna de la organización	Servicio	Todos los procesos de la organización	Medio
A18	Microsoft Dynamics 365 (CRM)	1	Gestión de clientes, emisión de pólizas, correo electrónico	Servicio	Comercial, Siniestros, Emisión, Proyectos	Alto
A19	Personal o Colaboradores	43	Personal que realiza funciones importantes dentro de la organización (gerentes, jefes, ejecutivos)	Personas	Todos los procesos de la organización	Alto
A20	Cintas de Respaldo	15	Cintas utilizadas para realizar copias de seguridad (respaldos) de los datos almacenados en el sistema AS/400	Equipo Informático	Operaciones-Soporte TI, Proyectos	Alto
A21	Antivirus	1	Software implementado para detectar, prevenir y eliminar programas maliciosos que pueden comprometer la seguridad de un equipo dentro de la organización	Software	Operaciones-Soporte TI	Alto

A22	Aplicaciones Web y Sistema AS400 para la gestión y la emisión de pólizas	4	Sistemas informáticos que permiten la emisión y la gestión de pólizas en la organización	Software	Operaciones-Soporte TI, Proyectos	Alto

Tabla 1. Clasificación y evaluación de los activos de información

4.3.3 Evaluación de Riesgos

Durante la evaluación de riesgos, se deben considerar diferentes aspectos para obtener una visión completa de la situación de seguridad. Esto implica realizar un análisis en profundidad de los activos de información, los sistemas, las redes y las aplicaciones utilizadas por Seguros Alianza S.A.

Al llevar a cabo una evaluación exhaustiva de riesgos, Seguros Alianza S.A. estará en una posición sólida para tomar decisiones informadas sobre las medidas de seguridad necesarias. Esto incluye la implementación de controles adicionales, la actualización de políticas y procedimientos de seguridad, la mejora de la capacitación en ciberseguridad para el personal y la asignación de recursos adecuados para abordar las áreas de mayor riesgo.

En conclusión, la evaluación de riesgos es un componente crucial de nuestra investigación sobre la línea base de ciberseguridad de Seguros Alianza S.A. Al identificar y comprender las amenazas y vulnerabilidades, la organización podrá tomar medidas proactivas para proteger sus activos de información críticos y garantizar la seguridad de sus operaciones.

4.3.3.1 Dimensiones de la Seguridad de Información

Con el propósito de lograr una clasificación precisa de los activos de información de Seguros Alianza S.A., se utilizaron las dimensiones de la seguridad de la información

como referencia. Estas dimensiones, fundamentales para la protección de nuestros datos, se centran en tres pilares: confidencialidad, integridad y disponibilidad.

4.3.3.2 Consideraciones Utilizadas para Evaluar los Activos

Para valorar los activos de la organización, se han implementado escalas de tres valores que permiten evaluar y considerar los siguientes aspectos:

- Se ha establecido una escala uniforme para todas las dimensiones con el propósito de comparar los riesgos de manera equitativa.
- Escalas que permiten diferenciar los valores.

PILAR	VALOR	CLASE	DESCRIPCIÓN
Confidencialidad	1	Información Pública	Datos que podrían ser compartidos con entidades externas.
	2	Información Privada	Datos que únicamente pueden ser divulgados al personal interno de la compañía. En caso de que esta información se comparta con agentes externos, no habría un impacto significativo en las operaciones empresariales.
	3	Información Restringida	Datos que se comparten exclusivamente con departamentos y partes específicas dentro de la entidad. Si esta información llega a ser divulgada a individuos no autorizados, podría generar un impacto considerable en las operaciones de la empresa.
Integridad	1	No requerida	Este dato se emplea con el propósito de realizar consultas.
	2	Requerida	Es necesario mantener la integridad de la información; no obstante, en caso de que su contenido sea alterado de manera fraudulenta, las operaciones no sufrirían un impacto significativo.

	3	Obligatoria	La pérdida de integridad de esta información podría generar un déficit en el funcionamiento de las operaciones de la compañía.
Disponibilidad	1	Bajo	Los procedimientos de la compañía no resultan impactados en caso de que esta información no esté disponible.
	2	Medio	En caso de que la información no esté a disposición, podría haber un impacto en los procedimientos que hacen uso de ella. No obstante, existen enfoques alternativos para llevar a cabo las operaciones de manera contingente, o el proceso podría posponerse hasta que la información esté nuevamente disponible.
	3	Alto	La organización podría experimentar consecuencias graves en sus procesos si la información no está disponible cuando se requiere.

Tabla 2. Valoración de los activos de información

4.3.3.3 Consideraciones Utilizadas para Evaluar las Amenazas

Para evaluar las amenazas, se emplearán dos criterios, los cuales consistirán en:

- Deterioro de un recurso o activo
- Probabilidad de Ocurrencia

Las amenazas serán clasificadas en tres categorías:

- Alta
- Media
- Baja

CRITERIO	VALOR	CATEGORÍA	DESCRIPCIÓN
Deterioro de un recurso o activo	1	Bajo	En caso de que la amenaza se materialice, el activo no experimentaría un deterioro significativo.
	2	Medio	Si la amenaza se presenta, el activo sufriría una degradación de tipo habitual.
	3	Alto	En caso de que la amenaza se materialice, el activo sufriría un deterioro severo.
Probabilidad de Ocurrencia	1	Bajo	La probabilidad es escasa, con una frecuencia de acontecimiento de una vez al año o menos.
	2	Medio	La probabilidad es moderada, con una frecuencia de ocurrencia de una vez cada seis meses o menos.
	3	Alto	La probabilidad es elevada, con una frecuencia de ocurrencia de una vez al mes o más.

Tabla 3. Evaluación de amenazas

4.3.3.4 Consideraciones Utilizadas para Evaluar la Vulnerabilidad

Para evaluar las vulnerabilidades, es necesario considerar el control de seguridad implementado.

Las vulnerabilidades serán clasificadas en tres categorías:

- Alta
- Media
- Baja

CRITERIO	VALOR	CATEGORÍA	DESCRIPCIÓN
Controles de Seguridad Implementados	1	Alto	Medidas establecidas y apropiadas para contrarrestar la amenaza
	2	Medio	Control de seguridad medio
	3	Bajo	Limitados o nulos controles de seguridad.

Tabla 4. Criterio para evaluar la vulnerabilidad

4.3.3.5 Reconocimiento de Amenazas y Vulnerabilidades

4.3.3.5.1 Reconocimiento de Amenazas

El propósito de este punto es detectar las potenciales amenazas que puedan existir dentro de Seguros Alianza S.A. y las vulnerabilidades que podrían ser aprovechadas por dichas amenazas. A continuación, describiremos las principales amenazas.

4.3.3.5.1.1 Amenazas de Procedencia Natural

AMENAZA	ACTIVOS AFECTADOS	VULNERABILIDAD
Fuego	Dispositivos informáticos, información sensible, infraestructura tecnológica, documentos físicos, energía eléctrica	Carencia de medidas de seguridad contra incendios
Agua	Dispositivos informáticos, información sensible, infraestructura tecnológica, documentos físicos, energía eléctrica	Ausencia de salvaguardias estructurales frente al agua.
Desastre Natural (Terremotos)	Dispositivos informáticos, información sensible, infraestructura tecnológica, documentos físicos, instalaciones, energía eléctrica	Problemas origen estructural presentes en la ubicación del activo.

Tabla 5. Amenazas de procedencia natural

4.3.3.5.1.2 Amenazas de Procedencia Industrial

AMENAZA	ACTIVOS AFECTADOS	VULNERABILIDAD
Suspensión del Suministro Eléctrico	Dispositivos informáticos, infraestructura tecnológica, redes de comunicaciones	Operación inapropiada de los sistemas de alimentación ininterrumpida (UPS)
Condiciones Inapropiadas de Temperatura	Dispositivos informáticos, infraestructura tecnológica, redes de comunicaciones	Deficiencias en el rendimiento del sistema de climatización de la empresa

Tabla 6. Amenazas de procedencia industrial

4.3.3.5.1.3 Amenazas involuntarias generadas por las acciones de las personas

AMENAZA	ACTIVOS AFECTADOS	VULNERABILIDAD
Errores de Usuarios	Dispositivos informáticos, servicios, información sensible, redes de comunicaciones	Falta de capacitación a los usuarios
Propagación de programas informáticos perjudiciales	Dispositivos informáticos, servicios, información sensible, redes de comunicaciones	Ausencia o deficiencia del software antivirus
Fugas de Información	Dispositivos informáticos, servicios, información sensible, redes de comunicaciones	Ausencia de medidas de garantía de la seguridad de la información
Vulnerabilidades en los programas informáticos	Dispositivos informáticos, servicios, información sensible, redes de comunicaciones	Inconvenientes relacionados con la actualización del software o que el software presente errores, fallos o problemas
La inoperatividad del sistema debido a los bajos recursos	Dispositivos informáticos, servicios, información sensible, redes de comunicaciones	Equipos informáticos con especificaciones mínimas necesarias para llevar a cabo la tarea

Tabla 7. Amenazas involuntarias

4.3.3.5.2 Reconocimiento de Vulnerabilidades

En las siguientes tablas se realizará la identificación de las vulnerabilidades que poseen los diferentes activos con sus respectivas amenazas que pueden llegar a ser un riego considerable para la organización.

4.3.3.5.2.1 Vulnerabilidades Tipo de Activo – Equipos Informáticos

TIPO DE ACTIVO – EQUIPOS INFORMÁTICOS	
AMENAZA	**VULNERABILIDAD**
Fuego	Ausencia de medidas de seguridad contra incendios
Afectaciones por Agua	Deficiencia en la salvaguarda estructural contra la filtración de agua
Afectaciones por Desastres Naturales (Terremoto)	Deficiencias estructurales en el edificio que alberga el activo
Inadecuaciones en el mantenimiento y la actualización de los equipos	Insuficiente o inexistente gestión de actualización de equipos.
Interrupción de la fuente de energía eléctrica	Operación deficiente de los sistemas de alimentación ininterrumpida (UPS).
Ambiente no apropiado en términos de temperatura y humedad	Deficiencias en el rendimiento del sistema de climatización en la organización
Hurto	Ausencia de sistemas de registro para supervisar la entrada y salida de recursos en la organización

Tabla 8. Vulnerabilidades equipos informáticos

4.3.3.5.2.2 Vulnerabilidades Tipo de Activo - Software

TIPO DE ACTIVO – SOFTWARE	
AMENAZA	**VULNERABILIDAD**
Fallas o equivocaciones por parte de los usuarios	Ausencia de formación o capacitación
Propagación de software malicioso	Carencia o ineficiencia en el antivirus

Divulgación de datos	La falta de medidas de aseguramiento de información
Vulnerabilidades en el software	Dificultades en la actualización o software con errores sin resolver
Alteración intencionada de los datos	Ausencia de protocolos y supervisión de modificaciones en los datos

Tabla 9. Vulnerabilidades software

4.3.3.5.2.3 Vulnerabilidades Tipo de Activo – Servicio

TIPO DE ACTIVO – SERVICIO	
AMENAZA	**VULNERABILIDAD**
Fallos en la recuperación de copias de seguridad	Carencia de protocolos para crear copias de seguridad y recuperarlas
Colapso del sistema debido al agotamiento de recursos	Dispositivos con recursos mínimas para realizar las tareas
Manipulación en la configuración	Ausencia de directrices de seguridad
Alteración intencionada de los datos	Deficiencia en la implementación de procedimientos y supervisión de modificaciones en la información

Tabla 10. Vulnerabilidades servicio

4.3.3.5.2.4 Vulnerabilidades Tipo de Activo – Redes de Comunicación

TIPO DE ACTIVO – REDES DE COMUNICACIÓN	
AMENAZA	**VULNERABILIDAD**
Fuego	Ausencia de medidas de seguridad contra incendios
Afectaciones por Agua	Deficiencia en la salvaguarda estructural contra la filtración de agua
Afectaciones por Desastres Naturales (Terremoto)	Deficiencias estructurales en el edificio que alberga el activo
Interrupción de la fuente de energía eléctrica	Operación deficiente de los sistemas de alimentación ininterrumpida (UPS).

Ambiente no apropiado en términos de temperatura y humedad	Deficiencias en el rendimiento del sistema de climatización en la organización

Tabla 11. Vulnerabilidades redes de comunicación

4.3.3.5.2.5 Vulnerabilidades Tipo de Activo – Personas

TIPO DE ACTIVO – PERSONAS	
AMENAZA	**VULNERABILIDAD**
Divulgación de datos	La falta de medidas de aseguramiento de información
Ausencia de los empleados	Escasa o inexistente supervisión del personal
Ingeniería social	Carencia de protocolos para acceder a la información.

Tabla 12. Vulnerabilidades personas

4.3.4 Políticas y Estándares de Seguridad

Dentro de nuestra investigación sobre la línea base de ciberseguridad de Seguros Alianza S.A., es esencial definir políticas y estándares de seguridad claros y comprensibles para la organización. Estas políticas establecen las directrices y normas que guían las prácticas de seguridad de la información en todos los niveles de la empresa. Al establecer políticas y estándares robustos, Seguros Alianza S.A. podrá fortalecer su postura de seguridad y garantizar la protección de sus activos de información críticos.

Es importante que las políticas y estándares de seguridad sean comunicados de manera efectiva a todos los empleados de Seguros Alianza S.A. Esto implica proporcionar capacitación inicial y continua, así como establecer mecanismos para garantizar el cumplimiento de las políticas.

A continuación, se detallan las políticas que deben abordar todo el entorno de seguridad dentro de la organización:

4.3.4.1 Política Para La Gestión de Contraseñas

Se deben establecer pautas claras sobre la creación y el manejo de contraseñas seguras. Esto incluye la elección de contraseñas robustas, la rotación periódica de contraseñas, la prohibición de compartir contraseñas y la implementación de mecanismos de autenticación multi factor.

Con el fin de garantizar la adecuada administración de la seguridad de las contraseñas, se aconseja a los usuarios considerar las siguientes directrices al crear y configurar contraseñas robustas:

- Las contraseñas deben contener letras mayúsculas y minúsculas, números y caracteres especiales.
- La contraseña debe tener al menos 8 caracteres de longitud como mínimo.
- Las contraseñas tienen una duración de 30 días, y el sistema requerirá automáticamente su modificación una vez que se cumpla ese período.
- La contraseña no debe incluir la denominación de la compañía, el nombre del usuario o términos que estén relacionados con el usuario.
- La cuenta de cualquier usuario que haya realizado tres intentos de acceso fallidos de forma consecutiva será suspendida.
- Cuando un usuario olvida su contraseña, deberá solicitar la asistencia de un técnico de soporte informático. Este profesional llevará a cabo el proceso para restablecer la contraseña y permitirá al usuario establecer una nueva desde su dispositivo la próxima vez que acceda al sistema.
- No se debe divulgar la contraseña a ningún otro usuario, ya que hacerlo implica que el usuario será responsable de las acciones que otros realicen con esa contraseña y se verá expuesto a las consecuencias correspondientes.
- El usuario no debe almacenar su contraseña en un formato que sea legible ni escribirla en papel y dejarla en lugares donde pueda ser descubierta.

- Los usuarios no deben tratar de infringir las medidas de seguridad y los sistemas de control de acceso. Cualquier acción de esta índole se considera una violación de las políticas de la organización.
- La modificación de la contraseña de un usuario que no está presente solo puede ser solicitada por el jefe inmediato o el director, con el fin de restablecerla y permitir la creación de una nueva.

4.3.4.2 Política de Acceso a los Sistemas

Las políticas deben definir los niveles de acceso a los sistemas y los procedimientos para otorgar, modificar o revocar privilegios de usuario. Esto incluye la implementación de controles de acceso basados en roles y la revisión regular de los derechos de acceso para garantizar que solo los usuarios autorizados tengan acceso a la información y los recursos adecuados.

Estas políticas están diseñadas para garantizar que el acceso a los sistemas informáticos sea seguro y controlado. A continuación, se describen los aspectos clave de las políticas de seguridad para el acceso a los sistemas:

- Ofrecer una interfaz que permita gestionar la autorización para acceder a las funciones de las aplicaciones del sistema.
- La asignación de accesos a las funciones será responsabilidad del titular de la información correspondiente.
- Se deberán crear perfiles o roles de acceso para las aplicaciones y sistemas, con el fin de asignarlos a los usuarios de manera efectiva, implementando así un control de acceso basado en roles.
- El acceso a un recurso solo será autorizado cuando sea justificado por una necesidad legítima relacionada con la actividad en desarrollo.
- Los usuarios solo deberán tener los permisos esenciales y mínimos concedidos.
- Es necesario garantizar una apropiada separación de tareas para crear y asignar privilegios de acceso.

- Ningún usuario podrá acceder a un sistema de información bajo control sin la aprobación del responsable del usuario en cuestión.
- Supervisar los permisos de acceso de los usuarios, que pueden incluir autorización para leer, escribir, eliminar y ejecutar acciones específicas.

4.3.4.3 Política de Protección de Datos

Las políticas deben establecer las medidas necesarias para proteger la confidencialidad, integridad y disponibilidad de los datos. Esto puede incluir el cifrado de datos sensibles, la implementación de controles de acceso y la adopción de prácticas de respaldo y recuperación de datos.

- Garantizar la confidencialidad de la información de autenticación, manteniendo su secreto y evitando su divulgación a terceros, incluyendo a personas con autoridad.
- Prevenir la retención de un registro ya sea en forma física, archivo de software o dispositivo móvil de la información de autenticación confidencial.
- Modificar la información de autenticación confidencial en caso de sospechar que podría haber sido comprometida o descubierta por partes no autorizadas.
- No se debe divulgar la información de autenticación confidencial de un usuario a terceros.
- No se debe emplear la información de autenticación confidencial para propósitos que no estén directamente relacionados con las operaciones de Seguros Alianza S.A., como, por ejemplo, en cuentas personales de redes sociales, bancos, establecimientos comerciales, entre otros.
- El departamento de Tecnologías de Información tiene la responsabilidad de supervisar la adecuada realización de las copias de seguridad y su posterior restauración, así como de generar los registros pertinentes.
- Se requiere que todos los datos digitales, programas y sistemas que se respaldan en Seguros Alianza S.A. sean guardados en una ubicación física que

esté separada de las salas de servidores a una distancia adecuada, con el propósito de prevenir posibles daños en caso de desastres; esta ubicación se designará como el lugar donde los expertos controlan las cintas.

- Las cintas de copia de seguridad deberán ser almacenadas en un entorno físico y ambiental apropiado con el fin de preservar la confidencialidad, integridad y disponibilidad de la información digital, software y sistemas informáticos.
- El acceso al área de almacenamiento de las copias de seguridad estará limitado, permitiéndose únicamente al personal autorizado por la Unidad de Tecnologías de la Información.
- En el plan de contingencia, es esencial tener en cuenta la realización de pruebas de restauración de copias de seguridad efectuadas en ciclos previos.

4.3.4.4 Política de Prácticas de Seguridad en el Lugar de Trabajo

Las políticas deben abordar las prácticas de seguridad que se deben seguir en el entorno de trabajo. Esto puede incluir el bloqueo automático de dispositivos después de un período de inactividad, la protección física de los dispositivos y la promoción de la conciencia de seguridad entre los empleados.

- El usuario debe asegurarse de que, cada vez que se aleje de su estación de trabajo, bloquee la sesión de su computadora para prevenir accesos no autorizados.
- Es necesario salvaguardar tanto física como digitalmente los dispositivos pertenecientes a Seguros Alianza S.A. para prevenir el robo, el acceso no autorizado o la divulgación de información. En situaciones apropiadas, se llevará a cabo el cifrado de los datos y se realizarán copias de seguridad.
- Si un equipo asignado se extravía o es robado, el usuario tendrá la responsabilidad de notificar de inmediato a la organización y al encargado de Tecnologías de la Información (T.I.) con el fin de tomar de manera pronta y apropiada las medidas de seguridad necesarias para proteger la información contenida.

- El usuario debe mantenerse en proximidad constante de los dispositivos asignados en todo momento.
- El usuario no debe descuidar los equipos.
- Evitar destacar o hacer evidente que se está llevando consigo un equipo valioso.
- No colocar etiquetas o identificaciones de Seguros Alianza S.A. en el dispositivo, excepto aquellas que sean imprescindibles.
- No agregar información de contacto técnico en el dispositivo.

4.3.5 Controles de Seguridad

Dentro del marco de nuestra investigación sobre la línea base de ciberseguridad de Seguros Alianza S.A., es fundamental establecer controles de seguridad adecuados para mitigar los riesgos identificados. Estos controles representan las medidas y soluciones técnicas que se implementan con el fin de proteger los activos de información críticos de la organización. Al implementar controles de seguridad efectivos, Seguros Alianza S.A. podrá reducir la exposición a amenazas y minimizar el impacto de posibles incidentes de seguridad.

A continuación, se mencionan algunos de los controles de seguridad que se encuentran implementados dentro de la organización:

4.3.5.1 Firewall

El despliegue de un firewall es esencial para proteger la infraestructura tecnológica de Seguros Alianza S.A. Este dispositivo actúa como una barrera entre las redes internas y externas, filtrando el tráfico no deseado y bloqueando los ataques maliciosos. Los firewalls pueden configurarse para aplicar políticas de seguridad específicas y monitorear continuamente el tráfico en busca de posibles amenazas.

Para Seguros Alianza S.A. se estableció e implementó un firewall de Fortinet, el cual es un componente crucial de la infraestructura de seguridad de red diseñado para proteger la red y los sistemas de la organización contra amenazas cibernéticas. Fortinet es conocido por su amplia gama de productos de seguridad, y su firewall combina hardware y software para proporcionar una defensa integral contra amenazas en línea. A continuación, se presenta las características y capacidades clave de un firewall de Fortinet:

- **Inspección de Paquetes:** El firewall de Fortinet realiza una inspección profunda de paquetes, lo que significa que analiza el tráfico de red a nivel de paquete para detectar y bloquear amenazas, como programas malignos, intrusiones y ataques de denegación de servicio.
- **Filtrado de Contenido:** Puede filtrar el contenido web, lo que permite a la empresa aplicar políticas de acceso a Internet, bloquear sitios web maliciosos o inapropiados y prevenir la pérdida de datos confidenciales.
- **VPN Segura:** Facilita la creación de conexiones VPN seguras para permitir a los empleados acceder a la red de la empresa de forma segura desde ubicaciones remotas.
- **Gestión de Amenazas Avanzadas:** Utiliza múltiples tecnologías de seguridad, como antivirus, antispam, filtrado de aplicaciones para proteger la red contra amenazas avanzadas y ataques sofisticados.
- **Gestión Centralizada:** Permite la administración centralizada de múltiples dispositivos FortiGate en toda la red de la empresa, lo que facilita la implementación y la aplicación de políticas de seguridad coherentes.
- **Informes y Análisis:** Proporciona informes detallados sobre el tráfico de red y las amenazas detectadas, lo que permite a los administradores evaluar la eficacia de las políticas de seguridad.

- **Alta Disponibilidad:** Puede configurarse en modos de alta disponibilidad para garantizar la continuidad operativa y la redundancia en caso de fallos.
- **Escalabilidad:** Escala de manera efectiva para adaptarse al crecimiento de la red de la empresa, lo que lo hace adecuado para organizaciones de diferentes tamaños.

4.3.5.2 Antivirus

Las soluciones de antivirus y antimalware son fundamentales para proteger los sistemas y dispositivos de Seguros Alianza S.A. Estas herramientas ayudan a detectar y eliminar software malicioso, como virus, troyanos y ransomware, que podrían comprometer la seguridad de los activos de información.

Para Seguros Alianza S.A. se estableció e implementó un antivirus de ESET, la cual es una herramienta de seguridad cibernética diseñada para proteger los sistemas y la infraestructura informática de la organización contra amenazas de programas malignos, virus y otros riesgos en línea. ESET es conocido por su amplia gama de soluciones de seguridad, y su antivirus es una parte esencial de su conjunto de productos de seguridad. A continuación, se presenta una descripción general de un antivirus de ESET:

- **Protección en Tiempo Real:** El antivirus ESET ofrece una protección constante y en tiempo real contra virus, programas malignos, ransomware, troyanos y otros tipos de amenazas cibernéticas. Detecta y bloquea activamente las amenazas antes de que puedan causar daño.
- **Filtrado de Contenido Web:** Permite a la empresa establecer políticas de acceso a Internet, bloquear sitios web maliciosos o inapropiados y prevenir la pérdida de datos confidenciales a través de la supervisión y el filtrado de contenido web.
- **Actualizaciones Automáticas:** Mantiene las bases de datos de firmas de virus y las definiciones de amenazas actualizadas de forma automática, lo que garantiza una protección continua contra las últimas amenazas.

- **Exploración Programada:** Permite programar exploraciones periódicas de los sistemas y dispositivos para buscar y eliminar programas malignos y otras amenazas ocultas.
- **Protección de Correo Electrónico:** Analiza los correos electrónicos y los archivos adjuntos en busca de programas maliciosos y amenazas antes de que puedan infectar la red.
- **Mínimo Impacto en el Rendimiento:** ESET Antivirus está diseñado para operar de manera eficiente sin ralentizar significativamente el rendimiento de los sistemas, lo que garantiza que los usuarios puedan trabajar de manera productiva.
- **Gestión Centralizada:** Permite a los administradores de TI gestionar y supervisar la seguridad de múltiples sistemas desde una consola centralizada, lo que facilita la implementación y la aplicación de políticas de seguridad coherentes.
- **Informes y Análisis:** Proporciona informes detallados sobre las actividades de seguridad, lo que permite a los administradores evaluar la eficacia de las políticas de seguridad y tomar medidas correctivas cuando sea necesario.
- **Compatibilidad Multiplataforma:** Es compatible con una variedad de sistemas operativos, incluyendo Windows, macOS y Linux, lo que lo hace versátil en entornos empresariales heterogéneos.

4.3.5.3 Autenticación Multifactorial

La implementación de la autenticación multifactorial es una medida de seguridad efectiva para proteger el acceso a los sistemas y aplicaciones de la organización. Al requerir múltiples formas de autenticación, como contraseñas, códigos de verificación y tokens, se añade una capa adicional de protección contra el acceso no autorizado.

Para Seguros Alianza S.A. se estableció e implementó la autenticación multifactorial (MFA) en Office 365, la cual es una capa adicional de seguridad diseñada para proteger las cuentas de usuario y los recursos de Microsoft 365 (anteriormente conocido como Office 365) contra accesos no autorizados. MFA requiere que los usuarios proporcionen múltiples formas de verificación antes de permitirles el acceso a sus cuentas y datos en línea. A continuación, se presenta una descripción general de la autenticación multifactorial de Office 365:

- **Autenticación de Dos o Más Factores:** MFA requiere que los usuarios proporcionen dos o más formas de autenticación antes de permitirles el acceso. Esto suele incluir algo que el usuario conoce (como una contraseña) y algo que el usuario tiene (como un dispositivo móvil).
- **Métodos de Verificación Variados:** Los métodos de verificación pueden incluir el uso de códigos de un solo uso enviados por SMS, aplicaciones de autenticación móvil, llamadas de voz, tarjetas de seguridad físicas u otras opciones personalizadas.
- **Seguridad Adicional para Contraseñas:** Dado que las contraseñas son vulnerables a robos o ataques de suplantación de identidad, MFA agrega una capa de protección significativa al requerir una segunda forma de autenticación.
- **Prevención de Accesos No Autorizados:** La MFA hace que sea mucho más difícil para los ciberdelincuentes acceder a cuentas, incluso si obtienen la contraseña de un usuario. Esto reduce el riesgo de accesos no autorizados y protege la información sensible.
- **Opciones de Configuración Avanzada:** Los administradores de Office 365 pueden configurar políticas de MFA personalizadas para adaptarse a las necesidades y la estructura de seguridad de su empresa. Esto incluye la capacidad de exigir MFA solo en ubicaciones específicas o para ciertos usuarios.
- **Informes y Auditoría:** Microsoft 365 proporciona registros detallados y reportes de seguridad para rastrear el uso de la MFA y detectar posibles amenazas o comportamientos sospechosos.

- **Compatibilidad con Aplicaciones y Servicios:** MFA se puede habilitar no solo para el acceso a Microsoft 365, sino también para proteger aplicaciones y servicios relacionados, como SharePoint, OneDrive y Teams.
- **Facilidad de Uso para Usuarios Finales:** Aunque agrega una capa de seguridad, MFA se ha diseñado para ser relativamente conveniente para los usuarios finales, a menudo con opciones de "Recordarme" y configuraciones de confianza.

4.3.5.4 Cifrado de Datos

El cifrado de datos es fundamental para proteger la confidencialidad de la información sensible. Mediante el uso de algoritmos criptográficos, los datos se convierten en un formato ilegible para cualquier persona no autorizada. Esto proporciona una capa adicional de seguridad, incluso si los datos son interceptados o comprometidos.

Para Seguros Alianza S.A. se estableció e implementó el cifrado de datos con GAM (GeneXus Access Manager) lo cual es una medida de seguridad esencial destinada a proteger la información y los recursos sensibles que se gestionan a través de aplicaciones desarrolladas con GeneXus. GAM es una herramienta de seguridad de acceso y gestión de usuarios que permite a las empresas controlar y administrar quién tiene acceso a qué datos y funcionalidades en sus aplicaciones. El cifrado de datos en este contexto implica la protección de la información confidencial, como credenciales de usuario y datos críticos, mediante técnicas de cifrado avanzadas. A continuación, se presenta una descripción general del cifrado de datos en GAM GeneXus:

- **Cifrado de Datos en Reposo:** El cifrado de datos se aplica a los datos almacenados en reposo, como contraseñas de usuarios, información de perfil, registros de auditoría y otros datos sensibles. Esto asegura que, incluso si un atacante accede a la base de datos, los datos permanecen inaccesibles sin la clave de descifrado.

- **Cifrado de Datos en Tránsito:** Además de cifrar los datos en reposo, se cifra el tráfico de datos entre los clientes y el servidor. Esto protege la información mientras se transmite a través de la red y previene la interceptación de datos por parte de atacantes.
- **Gestión de Claves Segura:** El sistema de cifrado de datos en GAM GeneXus debe contar con una gestión segura de claves. Esto incluye la generación y el almacenamiento seguro de claves criptográficas, así como la gestión de políticas de rotación de claves.
- **Integración con GAM:** El cifrado de datos se integra estrechamente con GAM para garantizar que solo usuarios autorizados puedan descifrar y acceder a la información cifrada. GAM proporciona políticas de acceso y control de usuarios, lo que permite definir quién tiene derecho a descifrar datos específicos.
- **Auditoría y Registro de Eventos:** El sistema registra eventos de cifrado y descifrado, lo que permite realizar un seguimiento de las actividades relacionadas con la seguridad. Esto es fundamental para la conformidad y la detección de intentos de acceso no autorizado.
- **Capacitación y Concienciación del Personal:** Es importante capacitar a los usuarios y al personal de TI sobre las políticas de seguridad y la importancia del cifrado de datos para garantizar una implementación eficaz.

Además de los controles mencionados anteriormente, es importante destacar que los controles de seguridad deben ser revisados y actualizados de forma periódica para adaptarse a las nuevas amenazas y vulnerabilidades que puedan surgir. También se debe considerar la implementación de controles específicos para aplicaciones web, como escaneo de vulnerabilidades, filtrado de contenido y protección contra ataques de inyección de código.

En conclusión, la implementación de controles de seguridad sólidos es fundamental para proteger la infraestructura tecnológica y los activos de información críticos de

Seguros Alianza S.A. Estos controles trabajan en conjunto para mitigar los riesgos identificados y garantizar la seguridad de las operaciones de la organización. Al combinar medidas técnicas y políticas adecuadas, Seguros Alianza S.A. estará en una mejor posición para hacer frente a las amenazas cibernéticas y mantener un entorno seguro para sus activos de información.

4.3.6 Educación y Capacitación

Dentro del alcance de nuestra investigación sobre la línea base de ciberseguridad de Seguros Alianza S.A., es esencial destacar la importancia de la educación y capacitación en ciberseguridad. La concienciación y la formación de los empleados son elementos fundamentales para fortalecer la postura de seguridad de la organización. Al educar a los colaboradores sobre las mejores prácticas de seguridad y fomentar una cultura de seguridad, Seguros Alianza S.A. podrá reducir significativamente el riesgo de violaciones de seguridad causadas por errores humanos y mejorar la protección de sus activos de información.

En Seguros Alianza S.A. se establecieron charlas y capacitaciones en Ciberseguridad en donde se abordaron temas de suma importancia como los siguientes aspectos clave que se detallan a continuación:

- **Concientización sobre amenazas:** Los colaboradores se encuentran informados sobre las diversas amenazas cibernéticas que existen, como el phishing, programas malignos, los ataques de ingeniería social y el ransomware. El enfoque principal se centró en la identificación y prevención de tales amenazas, proporcionando ejemplos prácticos junto con técnicas de detección.
- **Mejores prácticas de seguridad:** Los empleados recibieron capacitación sobre las mejores prácticas de seguridad que deben seguir en su trabajo diario. Esto incluye el uso seguro de contraseñas, la actualización regular de software y sistemas, la protección de datos confidenciales, la restricción de permisos y la adhesión a las políticas de seguridad establecidas.

- **Phishing y ataques de ingeniería social:** Los empleados fueron capacitados para reconocer y responder adecuadamente a los ataques de phishing y los intentos de ingeniería social. Esto implica que se les educó sobre las señales de advertencia de un correo electrónico o mensaje sospechoso, cómo verificar la autenticidad de los remitentes y cómo reportar posibles intentos de phishing a los equipos de seguridad.
- **Uso seguro de contraseñas:** En la capacitación se incluyó pautas claras sobre la creación y el manejo seguro de contraseñas. Los empleados ahora son conscientes de la importancia de utilizar contraseñas robustas, únicas y de cambiarlas regularmente. Además, se enfatizó la importancia de no compartir contraseñas y utilizar autenticación multifactorial siempre que sea posible.
- **Protección de datos confidenciales:** Los empleados comprenden la importancia de proteger los datos confidenciales de la organización y seguir las políticas establecidas para su manejo adecuado. Para esto se realizó énfasis en el uso de cifrado, la clasificación correcta de la información, el acceso restringido a datos confidenciales y la notificación inmediata de cualquier incidente de seguridad.
- **Pruebas de conocimiento:** Además de la capacitación inicial, se realizaron pruebas periódicas para evaluar el nivel de conocimiento de los empleados en materia de ciberseguridad. Estas pruebas ayudaron a identificar brechas de conocimiento y áreas que requieren una mayor atención en términos de educación y capacitación.

Es importante que la educación y capacitación en ciberseguridad sean un proceso continuo y se actualicen regularmente para mantenerse al día con las últimas amenazas y mejores prácticas de seguridad. La creación de una cultura de seguridad en toda la organización, donde la seguridad cibernética sea una responsabilidad compartida, contribuirá en gran medida a fortalecer la línea base de ciberseguridad de Seguros Alianza S.A. y proteger sus activos de información críticos.

4.3.7 Gestión de Incidentes

Dentro del ámbito de nuestra investigación sobre la línea base de ciberseguridad de Seguros Alianza S.A., es esencial destacar la importancia de establecer un proceso claro y efectivo para la gestión de incidentes de seguridad. La capacidad de responder rápidamente a los incidentes y de minimizar su impacto en la organización es fundamental para garantizar la continuidad del negocio y proteger los activos de información críticos.

A continuación, se presentan aspectos clave que fueron establecidos en relación con la gestión de incidentes de seguridad:

- **Notificación de incidentes:** Se estableció un mecanismo claro y fácil de usar para que los empleados notifiquen los incidentes de seguridad que identifiquen. Los colaboradores pueden utilizar una línea directa y específica de soporte con el departamento de operaciones de T.I. y Seguridad como también un correo electrónico preparado con un formato en particular para el caso dirigido al departamento antes mencionado. La notificación temprana de incidentes permite una respuesta rápida y ayuda a evitar la propagación o el empeoramiento de los problemas de seguridad.
- **Análisis de incidentes:** Una vez notificado un incidente, se encuentra establecido personal calificado que conforman el equipo de operaciones de T.I. y Seguridad para analizar y evaluar la situación. Ellos se encargarán de investigar las causas raíz, determinar el alcance del incidente y evaluar el impacto en los activos de información y en la infraestructura tecnológica de la organización. El análisis de incidentes permite comprender la naturaleza del incidente y tomar decisiones informadas sobre las acciones a seguir.
- **Respuesta a incidentes:** Se definieron roles y responsabilidades claras para el equipo encargado de responder a los incidentes de seguridad. Este equipo se encuentra preparado y cuenta con los recursos necesarios para

abordar rápidamente el incidente, mitigar el daño y restablecer la normalidad. Se establecieron planes de respuesta predefinidos y cada determinado tiempo se practican ejercicios de simulación para garantizar una respuesta eficiente y coordinada.

- **Recuperación y mejora:** Después de abordar el incidente, se deberá llevar a cabo el proceso de recuperación que se implementó en la organización para restaurar los sistemas y los datos afectados a un estado seguro y funcional. Además, es importante aprovechar la experiencia adquirida para mejorar las medidas de seguridad existentes y prevenir futuros incidentes similares. Esto puede implicar actualizar las políticas y los controles de seguridad, mejorar la capacitación del personal y realizar ajustes en la infraestructura tecnológica.

ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE INCIDENTES		
	ROLES	**RESPONSABILIDADES**
ÁREA DE OPERACIONES DE T.I. Y SEGURIDAD	Administrador de Sistemas y Ejecutivo de Operaciones	Serán los responsables de ayudar a identificar y contener incidentes en sistemas y redes
	Analistas de Seguridad	Serán los responsables de ayudar en la evaluación de la seguridad, análisis de registros y detección de amenazas.
	Ingenieros de Seguridad	Serán los responsables de trabajar en la implementación de soluciones de seguridad, como cortafuegos, sistemas de detección de intrusiones y antivirus
	Administrador de Red y Ejecutivo de Operaciones	Serán los responsables de contribuir a la gestión de la red y la detección de anomalías en el tráfico.

Tabla 13. Roles y responsabilidades en gestión de incidentes

4.3.8 Mantenimiento y Actualizaciones de Sistemas y Software

Dentro del alcance de nuestra investigación sobre la línea base de ciberseguridad de Seguros Alianza S.A., es crucial destacar la importancia del mantenimiento y las actualizaciones regulares de los sistemas y el software utilizados por la organización. Mantener los sistemas actualizados con los últimos parches de seguridad y actualizaciones es fundamental para proteger los activos de información críticos y garantizar un entorno tecnológico seguro.

A continuación, se describen elementos fundamentales en relación con el mantenimiento y las actualizaciones de sistemas y software:

- **Parches de seguridad:** Los fabricantes de sistemas operativos, aplicaciones y software lanzan regularmente parches de seguridad para abordar las vulnerabilidades conocidas y corregir errores o debilidades en el código. Para este caso Seguros Alianza S.A. mantiene sus sistemas actualizados aplicando los parches de seguridad tan pronto como estén disponibles. Esto ayuda a cerrar las puertas a los posibles atacantes que podrían aprovechar las vulnerabilidades conocidas.
- **Actualizaciones de software:** Además de los parches de seguridad, las actualizaciones de software pueden incluir mejoras funcionales, correcciones de errores y nuevas características. Seguros Alianza S.A. se mantiene al día con las actualizaciones de los diferentes programas y aplicaciones que son utilizados. Las actualizaciones no solo mejoran la funcionalidad y el rendimiento del software, sino que también suelen incluir medidas de seguridad adicionales que fortalecen la protección de los activos de información.
- **Evaluación de compatibilidad:** Antes de aplicar cualquier actualización o parche, es importante realizar una evaluación de compatibilidad para

asegurarse de que no haya conflictos o incompatibilidades con otros componentes del sistema. Algunas actualizaciones pueden requerir ajustes o modificaciones adicionales para garantizar su funcionamiento correcto. Para este caso el área de operaciones de T.I. realiza pruebas en entornos controlados antes de implementar las actualizaciones en producción.

4.4 Plan De Remediación De Vulnerabilidades Identificadas

El Plan de Remediación de vulnerabilidades Identificadas para Seguros Alianza S.A es un componente crítico de la gestión de la seguridad de la información. Este proceso tiene como objetivo abordar y solucionar las debilidades o vulnerabilidades que se han identificado para las aplicaciones web o activos de tecnología de la información de la organización. A continuación, se proporciona una descripción más detallada de este plan:

4.4.1 Identificación de Vulnerabilidades

Identificar las vulnerabilidades existentes es un proceso fundamental en la seguridad informática y la gestión de riesgos cibernéticos. Esta actividad implica un análisis exhaustivo de sistemas, redes, aplicaciones y entornos tecnológicos con el objetivo de detectar posibles debilidades o fallos que podrían ser aprovechados por ciberdelincuentes o causar problemas de seguridad.

Para iniciar con la identificación de vulnerabilidades, se establecerán los servidores más críticos que Seguros Alianza S.A. tiene, para este caso se detallaran los servidores donde se encuentran alojados las aplicaciones web:

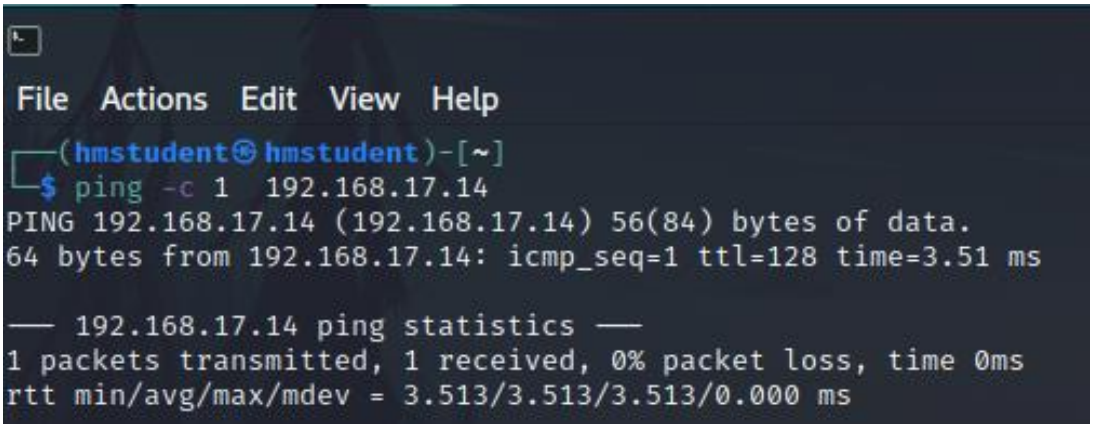
DIRECCIÓN IP	NOMBRE DE SERVIDOR	DESCRIPCIÓN
192.168.17.14	Autoclick	Emisión de pólizas y gestión
192.168.50.2	Oficina Virtual	Administración y gestión de siniestros
192.168.17.24	Autoclick Nueva Versión	Emisión de pólizas y módulos para usuarios internos
192.168.17.17	Facturación Electrónica	Gestión y autorización de documentos electrónicos
192.168.17.2	Incidencias	Administración y procesamientos de requerimientos

Tabla 14. Servidores críticos para analizar

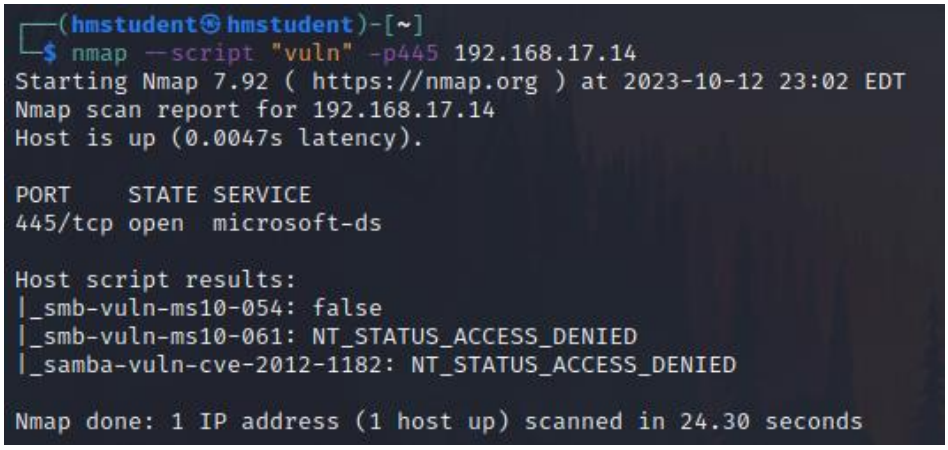
4.4.1.1 Servidor de Autoclick

Para la identificación de vulnerabilidades se utilizará Nmap, la cual es una poderosa herramienta de código abierto utilizada para realizar análisis de servidores, redes, descubrir dispositivos, identificar servicios en ejecución, mapear la topología de una red y, en particular, detectar vulnerabilidades en servidores. A continuación, se proporciona un detalle de cómo se utiliza Nmap para analizar el servidor de Autoclick de Seguros Alianza S.A.:

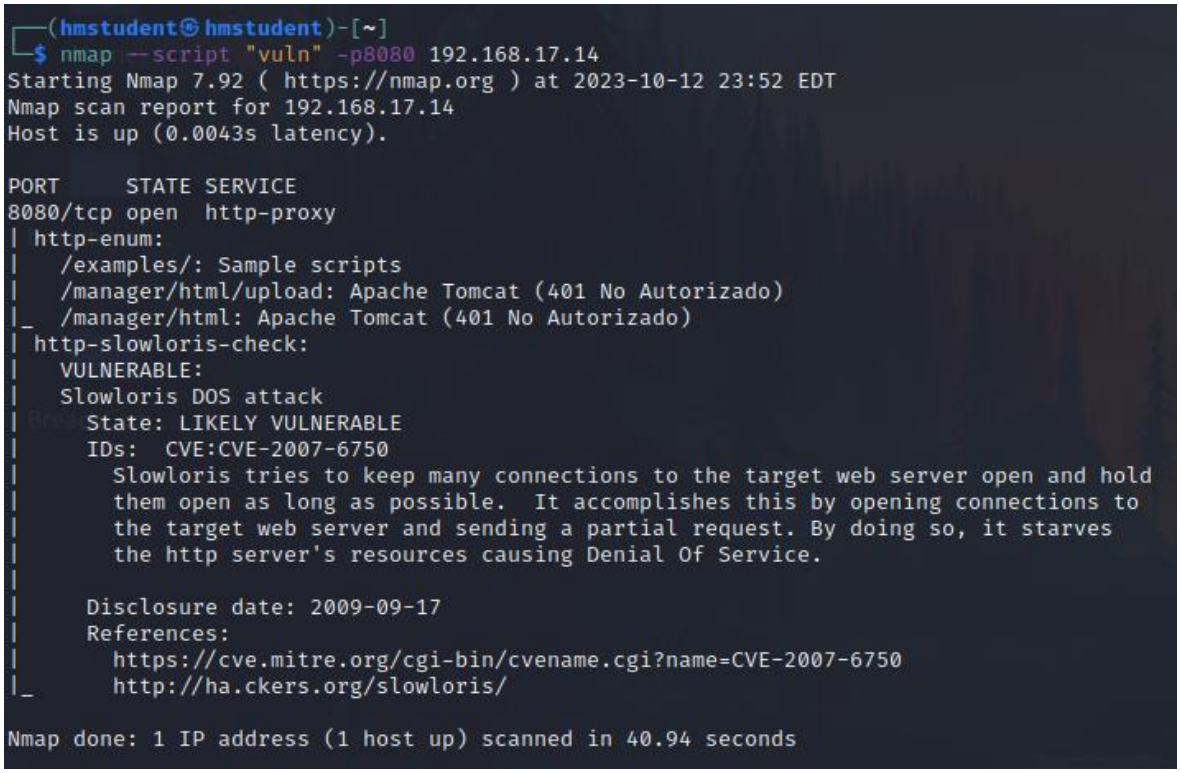
- Con el comando ping verificamos que tenemos conectividad desde el Kali Linux a la IP del servidor.



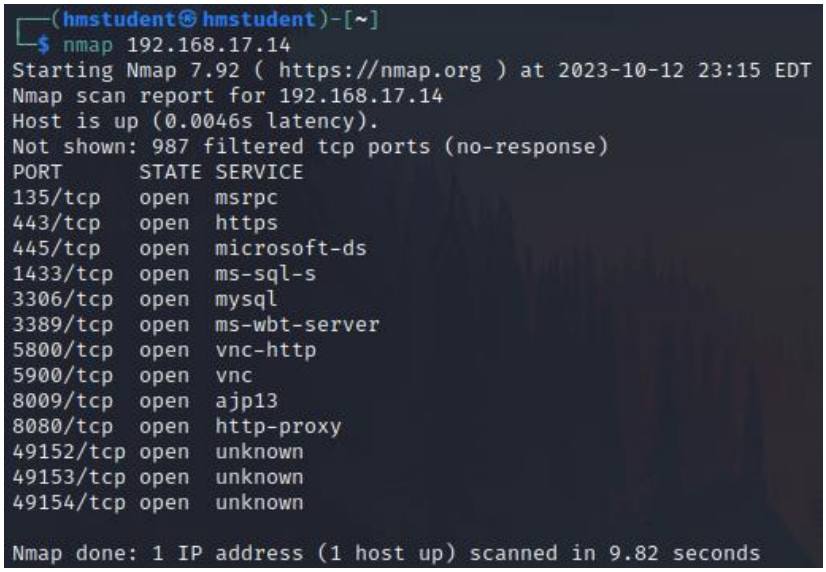
- Se realizó una búsqueda de vulnerabilidades con el puerto 445 y la dirección IP ya que es un servidor Windows en donde se encontró el puerto abierto.



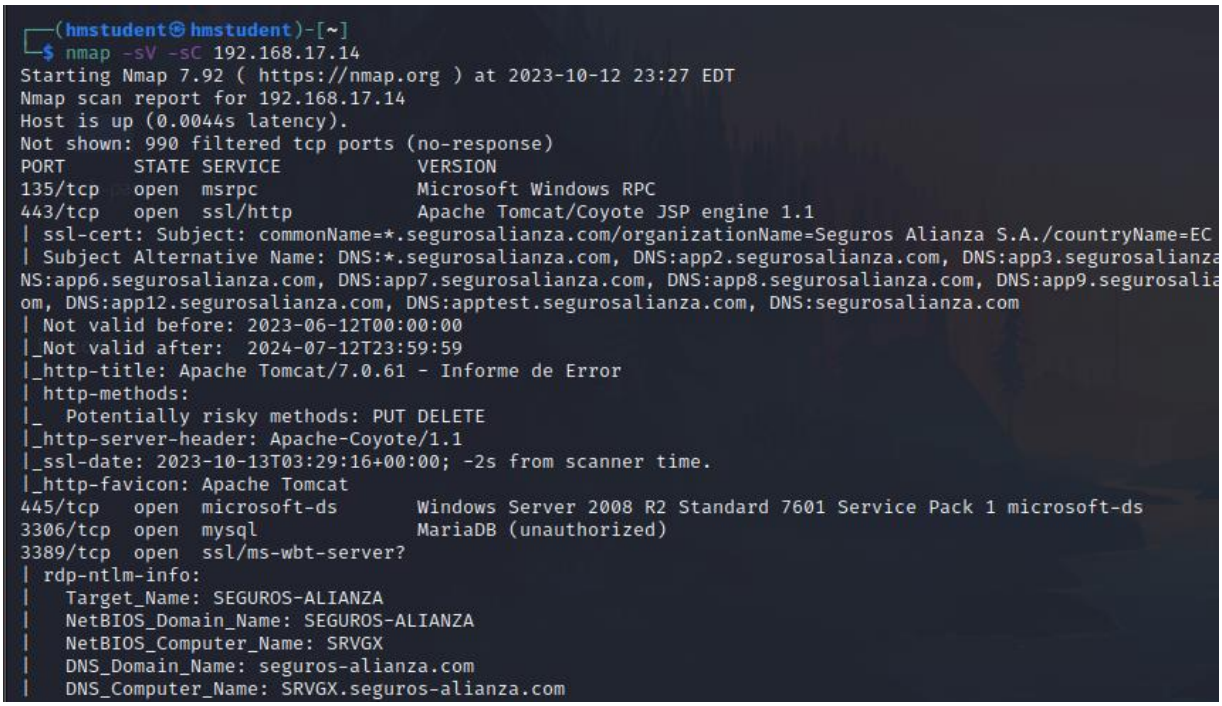
- Se realizó una búsqueda de vulnerabilidades con el puerto 8080 el cual corresponde a Apache Tomcat y la dirección IP del servidor, se encontró una vulnerabilidad (CVE-2007-6750).



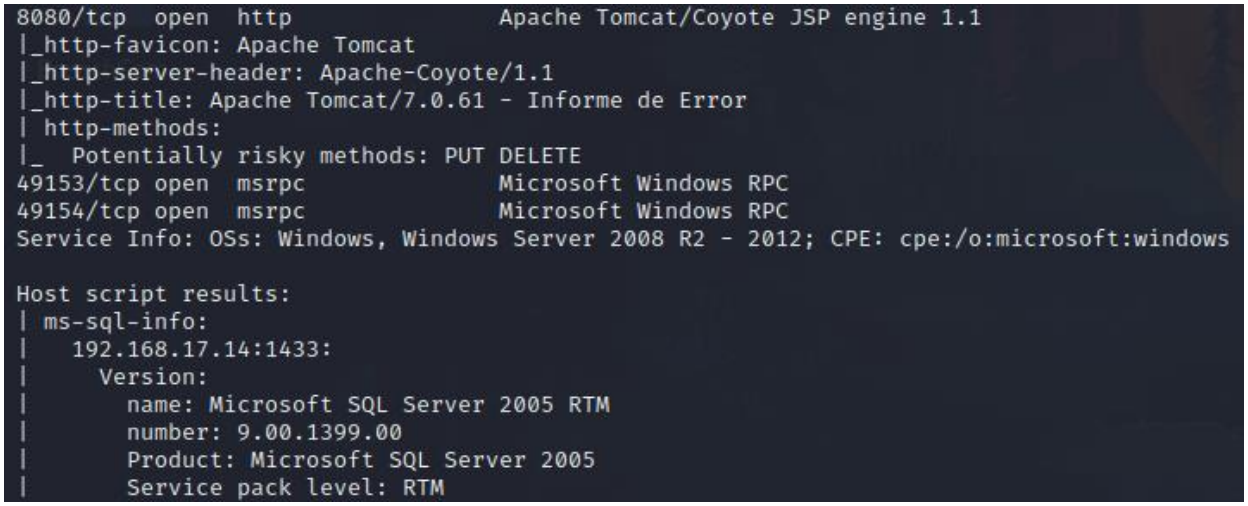
- Escaneo de todos los puertos que se encuentran abiertos en el servidor.



- En el escaneo y búsqueda de servicios en el servidor, se puede observar todos los DNS que tiene Seguros Alianza S.A., el servidor web con el que se trabaja para el desarrollo de aplicaciones web es Apache Tomcat, se encontraron varios puertos abiertos y el sistema operativo del servidor.

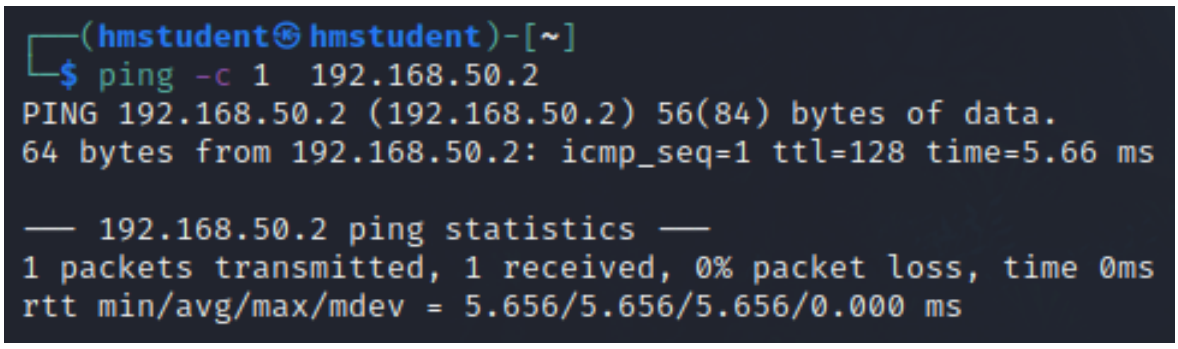


- El puerto 8080 correspondiente al servidor web Apache Tomcat se encuentra abierto, adicional que se puede saber la versión y el tipo de servidor de base de datos que está utilizando.



4.4.1.2 Servidor de Oficina Virtual

- Con el comando ping verificamos que tenemos conectividad desde el Kali Linux a la IP del servidor.



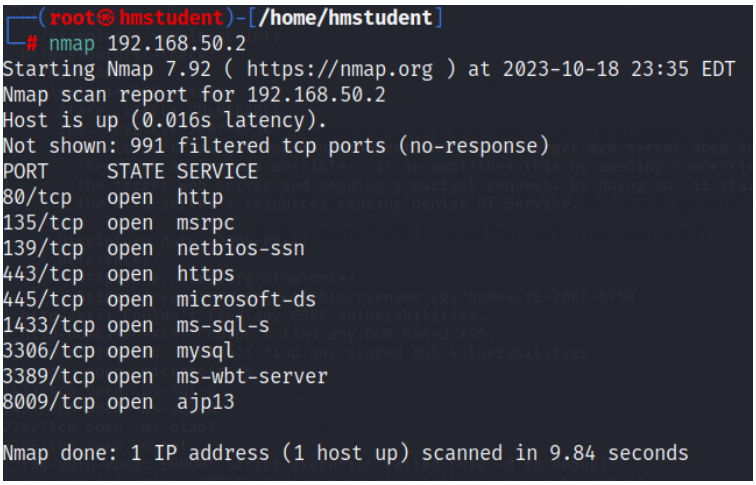
- Se realizó una búsqueda de vulnerabilidades con el puerto 445 y la dirección IP ya que es un servidor Windows en donde se encontró el puerto abierto.

```
┌──(hmstudent㉿hmstudent)-[~]
└─$ nmap --script "vuln" -p445 192.168.50.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-18 20:05 EDT
Nmap scan report for 192.168.50.2
Host is up (0.0058s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_samba-vuln-cve-2012-1182: No accounts left to try
|_smb-vuln-ms10-061: No accounts left to try
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 23.30 seconds
```

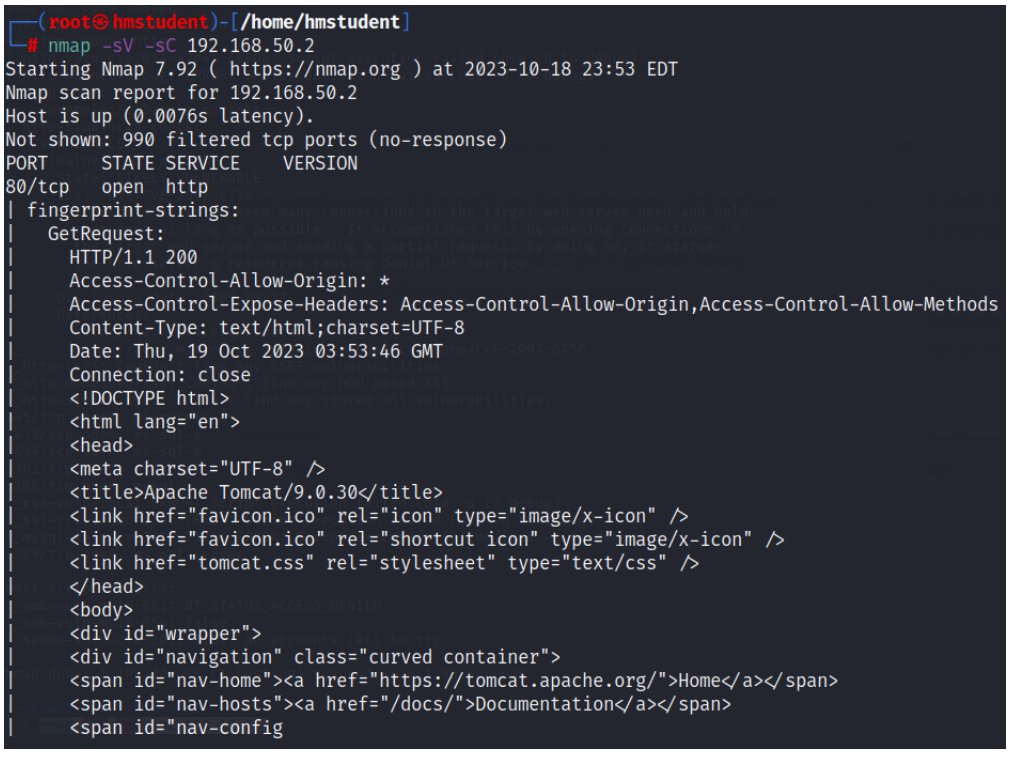
- Se realizó una búsqueda de vulnerabilidades con el puerto 80 el cual corresponde a Apache Tomcat y la dirección IP del servidor, se encontró una vulnerabilidad (CVE-2007-6750).

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p80 192.168.50.2

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-18 23:37 EDT
Nmap scan report for 192.168.50.2
Host is up (0.0017s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 615.41 seconds
```

- Escaneo de todos los puertos que se encuentran abiertos en el servidor.



- En el escaneo y búsqueda de servicios en el servidor, se puede observar todos los DNS que tiene Seguros Alianza S.A., el servidor web con el que se trabaja para el desarrollo de aplicaciones web es Apache Tomcat, se encontraron varios puertos abiertos e incluso la información del servidor de base de datos como su versión, puerto que utiliza y su service pack level.



```
139/tcp  open  tcpwrapped
443/tcp  open  tcpwrapped
| ssl-cert: Subject: commonName=*.segurosalianza.com/organizationName=Seguros Alianza S.A./countryName=EC
| Subject Alternative Name: DNS:*.segurosalianza.com, DNS:app2.segurosalianza.com, DNS:app3.segurosalianza.com,
 DNS:app6.segurosalianza.com, DNS:app7.segurosalianza.com, DNS:app8.segurosalianza.com, DNS:app9.segurosalianza.
za.com, DNS:app12.segurosalianza.com, DNS:apptest.segurosalianza.com, DNS:segurosalianza.com
| Not valid before: 2023-06-12T00:00:00
|_Not valid after:  2024-07-12T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/plain;charset=ISO-8859-1).
445/tcp  open  tcpwrapped
1434/tcp open  ms-sql-s   Microsoft SQL Server 2017 14.00.2047.00; RTM+
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2023-09-05T01:53:50
|_Not valid after:  2053-09-05T01:53:50
|_ssl-date: 2023-10-19T03:54:08+00:00; -1s from scanner time.
2382/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
3306/tcp open  tcpwrapped
3389/tcp open  tcpwrapped
|_ssl-date: 2023-10-19T03:54:07+00:00; -1s from scanner time.
| ssl-cert: Subject: commonName=ALIANZAappcloud
| Not valid before: 2023-09-08T13:53:22
|_Not valid after:  2024-03-09T13:53:22
| rdp-ntlm-info:
|   Target_Name: ALIANZAAPPCLOUD
|   NetBIOS_Domain_Name: ALIANZAAPPCLOUD
|   NetBIOS_Computer_Name: ALIANZAAPPCLOUD
|   DNS_Domain_Name: ALIANZAappcloud
|   DNS_Computer_Name: ALIANZAappcloud
|   Product_Version: 10.0.14393
|_  System_Time: 2023-10-19T03:53:52+00:00
8009/tcp open  tcpwrapped
```

```
Host script results:
|_clock-skew: mean: -1s, deviation: 0s, median: -1s
| ms-sql-info:
|   Windows server name: ALIANZAAPPCLOUD
|   192.168.50.2\SQLEXPRESS:
|     Instance name: SQLEXPRESS
|     Version:
|       name: Microsoft SQL Server 2017 RTM+
|       number: 14.00.2047.00
|       Product: Microsoft SQL Server 2017
|       Service pack level: RTM
|       Post-SP patches applied: true
|     TCP port: 1434
|     Clustered: false
|   192.168.50.2\SQLSERVER2019:
|     Instance name: SQLSERVER2019
|     Version:
|       name: Microsoft SQL Server 2019 GDR1+
|       number: 15.00.2101.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: GDR1
|       Post-SP patches applied: true
|     TCP port: 1433
|_    Clustered: false
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
```

4.4.1.3 Servidor Autoclick Nueva Versión

- Con el comando ping verificamos que tenemos conectividad desde el Kali Linux a la IP del servidor.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# ping -c 1  192.168.17.24
PING 192.168.17.24 (192.168.17.24) 56(84) bytes of data.
64 bytes from 192.168.17.24: icmp_seq=1 ttl=128 time=4.94 ms

── 192.168.17.24 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.938/4.938/4.938/0.000 ms
```

- Se realizó una búsqueda de vulnerabilidades con el puerto 445 y la dirección IP ya que es un servidor Windows en donde se encontró el puerto abierto.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p445 192.168.17.24

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 00:15 EDT
Nmap scan report for 192.168.17.24
Host is up (0.0014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_samba-vuln-cve-2012-1182: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-061: Could not negotiate a connection:SMB: Failed to receive bytes: ERROR
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 15.47 seconds
```

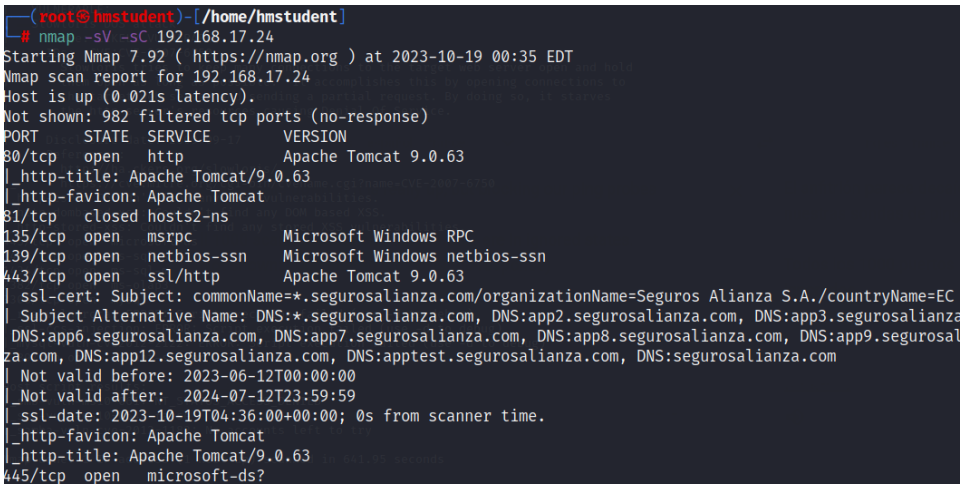
- Se realizó una búsqueda de vulnerabilidades con el puerto 80 el cual corresponde a Apache Tomcat y la dirección IP del servidor, se encontró una vulnerabilidad (CVE-2007-6750).

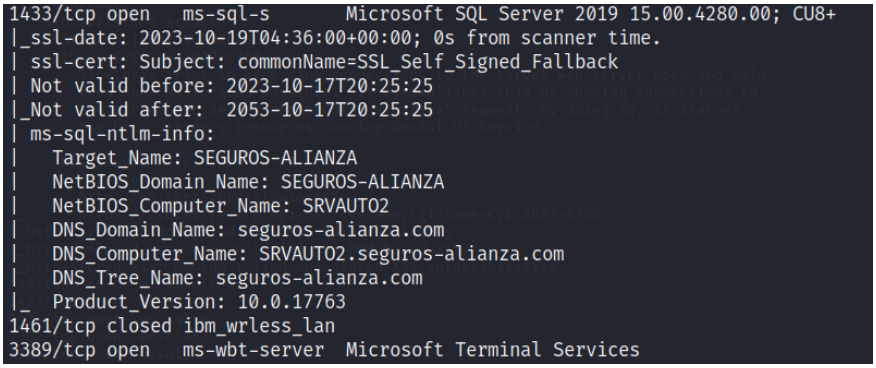
```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p80 192.168.17.24

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 00:19 EDT
Nmap scan report for 192.168.17.24
Host is up (0.00057s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.

Nmap done: 1 IP address (1 host up) scanned in 616.00 seconds
```

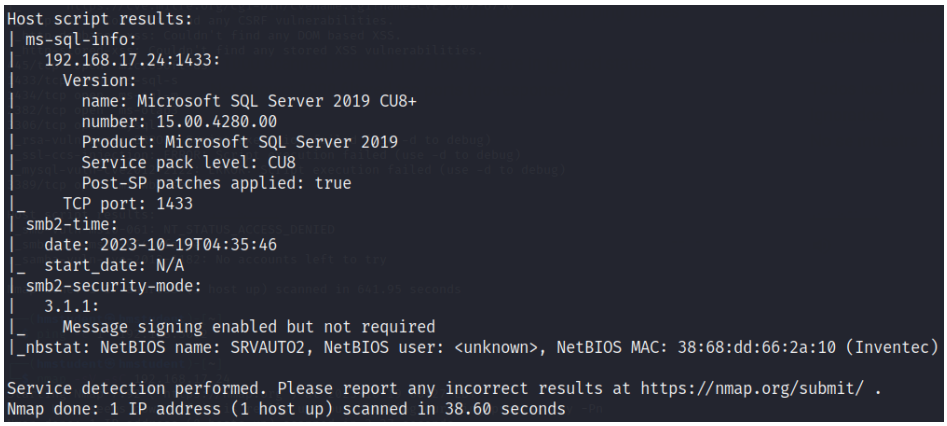
- Escaneo de todos los puertos que se encuentran abiertos en el servidor.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap 192.168.17.24
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 00:18 EDT
Nmap scan report for 192.168.17.24
Host is up (0.0032s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 4.88 seconds
```

- En el escaneo y búsqueda de servicios en el servidor, se puede observar todos los DNS que tiene Seguros Alianza S.A., el servidor web con el que se trabaja para el desarrollo de aplicaciones web es Apache Tomcat, se encontraron varios puertos abiertos e incluso la información del servidor de base de datos como su versión, puerto que utiliza y su service pack level.







4.4.1.4 Servidor de Facturación Electrónica

- Con el comando ping verificamos que tenemos conectividad desde el Kali Linux a la IP del servidor.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# ping -c 1  192.168.17.17
PING 192.168.17.17 (192.168.17.17) 56(84) bytes of data.
64 bytes from 192.168.17.17: icmp_seq=1 ttl=128 time=3.24 ms

── 192.168.17.17 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.238/3.238/3.238/0.000 ms
```

- Se realizó una búsqueda de vulnerabilidades con el puerto 445 y la dirección IP ya que es un servidor Windows en donde se encontró el puerto abierto.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p445 192.168.17.17

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 00:44 EDT
Nmap scan report for 192.168.17.17
Host is up (0.0014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 24.29 seconds
```

- Se realizó una búsqueda de vulnerabilidades con el puerto 80 el cual corresponde a Apache Tomcat y la dirección IP del servidor, se encontró una vulnerabilidad (CVE-2007-6750).

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p8080 192.168.17.17

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 00:57 EDT
Nmap scan report for 192.168.17.17
Host is up (0.0014s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy
| http-enum:
|   /examples/: Sample scripts
|   /manager/html/upload: Apache Tomcat (401 No Autorizado)
|   /manager/html: Apache Tomcat (401 No Autorizado)
|_  /docs/: Potentially interesting folder
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/

Nmap done: 1 IP address (1 host up) scanned in 57.56 seconds
```

- Escaneo de todos los puertos que se encuentran abiertos en el servidor.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap 192.168.17.17
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 00:59 EDT
Nmap scan report for 192.168.17.17
Host is up (2.1s latency).
Not shown: 985 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
139/tcp   open     netbios-ssn
443/tcp   open     https
445/tcp   open     microsoft-ds
514/tcp   filtered shell
2301/tcp  open     compaqdiag
2381/tcp  open     compaq-https
3306/tcp  open     mysql
3389/tcp  open     ms-wbt-server
8009/tcp  open     ajp13
8080/tcp  open     http-proxy
49152/tcp open     unknown
49153/tcp open     unknown
49154/tcp open     unknown
49156/tcp open     unknown

Nmap done: 1 IP address (1 host up) scanned in 694.02 seconds
```

- En el escaneo y búsqueda de servicios en el servidor, se puede observar todos los DNS que tiene Seguros Alianza S.A., el servidor web con el que se trabaja para el desarrollo de aplicaciones web es Apache Tomcat, se encontraron varios puertos abiertos e incluso la información del servidor de base de datos como su versión, puerto que utiliza y su service pack level.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap -sV -sC 192.168.17.17
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 01:18 EDT
Nmap scan report for 192.168.17.17
Host is up (0.018s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
443/tcp   open  ssl/http      Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.61
|_ssl-date: 2023-10-19T05:19:44+00:00; 0s from scanner time.
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
| ssl-cert: Subject: commonName=*.segurosalianza.com/organizationName=Seguros Alianza S.A./countryName=EC
| Subject Alternative Name: DNS:*.segurosalianza.com, DNS:app2.segurosalianza.com, DNS:app3.segurosalianza.com,
 DNS:app6.segurosalianza.com, DNS:app7.segurosalianza.com, DNS:app8.segurosalianza.com, DNS:app9.segurosalianza.
za.com, DNS:app12.segurosalianza.com, DNS:apptest.segurosalianza.com, DNS:segurosalianza.com
| Not valid before: 2023-06-12T00:00:00
|_Not valid after:  2024-07-12T23:59:59
445/tcp   open  microsoft-ds  Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds
2381/tcp  open  http          CompaqHTTPServer 9.9 (HP System Management)
```

```
3306/tcp  open  mysql         MySQL (unauthorized)
3389/tcp  open  ssl/ms-wbt-server?
|_ssl-date: 2023-10-19T05:19:44+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=SRVFACTELECT.seguros-alianza.com
| Not valid before: 2023-05-31T03:32:43
|_Not valid after:  2023-11-30T03:32:43
| rdp-ntlm-info:
|   Target_Name: SEGUROS-ALIANZA
|   NetBIOS_Domain_Name: SEGUROS-ALIANZA
|   NetBIOS_Computer_Name: SRVFACTELECT
|   DNS_Domain_Name: seguros-alianza.com
|   DNS_Computer_Name: SRVFACTELECT.seguros-alianza.com
|   DNS_Tree_Name: seguros-alianza.com
|   Product_Version: 6.1.7601
|_  System_Time: 2023-10-19T05:19:31+00:00
8009/tcp  open  ajp13         Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http          Apache Tomcat/Coyote JSP engine 1.1
```

```
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: SRVFACTELECT
|   NetBIOS computer name:
|   Domain name: seguros-alianza.com
|   Forest name: seguros-alianza.com
|   FQDN: SRVFACTELECT.seguros-alianza.com
|_  System time: 2023-10-19T00:19:31-05:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 134.54 seconds
```

4.4.1.5 Servidor de Incidencias

- Con el comando ping verificamos que tenemos conectividad desde el Kali Linux a la IP del servidor.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# ping -c 1  192.168.17.2
PING 192.168.17.2 (192.168.17.2) 56(84) bytes of data.
64 bytes from 192.168.17.2: icmp_seq=1 ttl=128 time=3.49 ms

── 192.168.17.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.489/3.489/3.489/0.000 ms
```

- Se realizó una búsqueda de vulnerabilidades con el puerto 445 y la dirección IP ya que es un servidor Windows en donde se encontró el puerto abierto.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p445 192.168.17.2

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 01:26 EDT
Nmap scan report for 192.168.17.2
Host is up (0.00085s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```

- Se realizó una búsqueda de vulnerabilidades con el puerto 80 el cual corresponde a Apache Tomcat y la dirección IP del servidor, se encontró una vulnerabilidad (CVE-2007-6750).

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap --script "vuln" -p8080 192.168.17.2

Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 01:42 EDT
Nmap scan report for 192.168.17.2
Host is up (0.0064s latency).

PORT     STATE SERVICE
8080/tcp open  http-proxy
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
| http-enum:
|   /manager/html/upload: Apache Tomcat (401 No Autorizado)
|   /manager/html: Apache Tomcat (401 No Autorizado)
|_  /docs/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 51.86 seconds
```

- Escaneo de todos los puertos que se encuentran abiertos en el servidor.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap 192.168.17.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 01:38 EDT
Nmap scan report for 192.168.17.2
Host is up (0.0024s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
5900/tcp open  vnc
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 20.45 seconds
```

- En el escaneo y búsqueda de servicios en el servidor, se puede observar todos los DNS que tiene Seguros Alianza S.A., el servidor web con el que se trabaja para el desarrollo de aplicaciones web es Apache Tomcat, se encontraron varios puertos abiertos.

```
┌──(root㉿hmstudent)-[/home/hmstudent]
└─# nmap -sV -sC 192.168.17.2
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-19 01:45 EDT
Nmap scan report for 192.168.17.2
Host is up (0.0019s latency).
Not shown: 992 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds  Windows Server (R) 2008 Standard 6003 Service Pack 2 microsoft-ds
3306/tcp open  mysql         MySQL 5.1.41
| tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
| tls-alpn: ERROR: Script execution failed (use -d to debug)
| ssl-date: ERROR: Script execution failed (use -d to debug)
| mysql-info:
|   Protocol: 10
|   Version: 5.1.41
|   Thread ID: 407
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, Speaks41ProtocolOld, LongPassword, FoundRows, SupportsCompression
|, SupportsLoadDataLocal, InteractiveClient, Speaks41ProtocolNew, ConnectWithDatabase, IgnoreSpaceBef
|   Status: Autocommit
|_  Salt: +t."_<LJk^vW20;wh#p.
| sslv2: ERROR: Script execution failed (use -d to debug)
3389/tcp open  ssl/ms-wbt-server?
```

```
3389/tcp open  ssl/ms-wbt-server?
| ssl-date: 2023-10-19T05:48:34+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=SrvAvital.seguros-alianza.com
| Not valid before: 2023-05-23T18:45:01
|_Not valid after:  2023-11-22T18:45:01
| rdp-ntlm-info:
|   Target_Name: SEGUROS-ALIANZA
|   NetBIOS_Domain_Name: SEGUROS-ALIANZA
|   NetBIOS_Computer_Name: SRVAVITAL
|   DNS_Domain_Name: seguros-alianza.com
|   DNS_Computer_Name: SrvAvital.seguros-alianza.com
|   DNS_Tree_Name: seguros-alianza.com
|   Product_Version: 6.0.6003
|_  System_Time: 2023-10-19T05:47:54+00:00
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5900/tcp open  vnc           VNC (protocol 3.6)
```

```
| rdp-ntlm-info:
|   Target_Name: SEGUROS-ALIANZA
|   NetBIOS_Domain_Name: SEGUROS-ALIANZA
|   NetBIOS_Computer_Name: SRVAVITAL
|   DNS_Domain_Name: seguros-alianza.com
|   DNS_Computer_Name: SrvAvital.seguros-alianza.com
|   DNS_Tree_Name: seguros-alianza.com
|   Product_Version: 6.0.6003
|_  System_Time: 2023-10-19T05:47:54+00:00
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
5900/tcp open  vnc           VNC (protocol 3.6)
| vnc-info:
|   Protocol version: 003.006
|   Security types:
|_    VNC Authentication (2)
8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/8.0.32
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 59m59s, deviation: 2h14m09s, median: 0s
| smb-os-discovery:
|   OS: Windows Server (R) 2008 Standard 6003 Service Pack 2 (Windows Server (R) 2008 Standard 6.0)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp2
```

4.4.2 Priorización de Vulnerabilidades

Es crucial llevar a cabo una clasificación detallada de las vulnerabilidades. Esta clasificación implica evaluar y categorizar cada vulnerabilidad en función de su gravedad y el riesgo que plantea para los activos de información de Seguros Alianza S.A. Esta fase es esencial para la gestión efectiva de la seguridad.

La priorización de vulnerabilidades según su gravedad y riesgo es una parte esencial de la gestión de la seguridad de la información. Esto permitirá a Seguros Alianza S.A. enfocar sus recursos de manera efectiva, abordando primero las amenazas más críticas y reduciendo así el riesgo general para sus activos de información.

Las vulnerabilidades se categorizarán de la siguiente manera:

CRÍTICA	Las vulnerabilidades deben ser consideradas como prioritarias para su corrección inmediata
ALTA	Las vulnerabilidades deben ser examinadas y solucionadas en cuanto sea factible
MEDIA	Las vulnerabilidades representan un riesgo mínimo para la integridad de los datos
BAJA	Esta clasificación abarca las vulnerabilidades que poseen un carácter informativo o preventivo

Tabla 15. Categorización de vulnerabilidades

- Vulnerabilidad CVE-2007-6750: Permite que atacantes remotos desencadenen una interrupción del servicio (denegación de servicio) al enviar solicitudes HTTP parciales, tal como se evidencia en el caso de Slowloris, en situaciones en las que falta el módulo mod_reqtimeout en versiones anteriores a la 2.2.15.
- Puerto 8080 Abierto: Tener el puerto 8080 de Apache Tomcat abierto en un servidor o sistema tiene ciertos riesgos asociados, ya que permite que el servidor web reciba solicitudes HTTP desde cualquier usuario o entidad en Internet.

A continuación, se detallan las vulnerabilidades encontradas y su categorización:

VULNERABILIDAD	CATEGORÍA	DESCRIPCIÓN
CVE-2007-6750	Media	Esta vulnerabilidad se la categoriza como media debido a que afecta solo a versiones anteriores a la 2.2.15 de Apache Tomcat y las aplicaciones web que Seguros Alianza S.A. utiliza las maneja con versiones superiores a la 7
Puertos abiertos (80, 8080, 445)	Alta	Esta vulnerabilidad se la categoriza como alta debido a que el tener puertos importantes abiertos expone a Seguros Alianza S.A. a diversos riesgos de seguridad y amenazas potenciales como ataques de fuerza bruta o denegación de servicio

Tabla 16. Vulnerabilidades encontradas

4.4.3 Evaluación del Impacto

La evaluación del impacto de vulnerabilidades es un proceso fundamental en la gestión de la seguridad de la información que implica analizar y comprender en detalle las posibles consecuencias y efectos negativos que podrían surgir a partir de las vulnerabilidades identificadas en las aplicaciones web o entorno de TI de Seguros Alianza S.A.

Esta evaluación tiene como objetivo proporcionar una base sólida para tomar decisiones informadas sobre cómo abordar y mitigar estas vulnerabilidades.

A continuación, se detalla una tabla con el impacto de las vulnerabilidades para Seguros Alianza S.A.:

IMPACTO DE VULNERABILIDADES EN SEGUROS ALIANZA S.A.	
VULNERABILIDAD	**IMPACTO**
CVE-2007-6750	• Denegación de Servicio
Puertos abiertos (80, 8080) de Apache Tomcat	• Exposición de la consola de administración • Escaneo y reconocimiento de red • Ataques de fuerza bruta • Consumo de recursos
Puertos abiertos (445)	• Exposición a ataques de red • Riesgo de programas malignos y ransomware • Inyección de programas malignos en recursos compartidos

Tabla 17. Impacto de vulnerabilidades

4.4.4 Desarrollo de soluciones

Después de establecer una jerarquía de las vulnerabilidades, es necesario idear respuestas o acciones de mitigación para resolverlas. Para este caso y en base a las vulnerabilidades que fueron encontradas y mitigadas se establece la actualización de software y la incorporación de controles de seguridad adicionales.

- Como medida de seguridad se realizó una planificación para poder actualizar el sistema operativo de los servidores que se les consideraron como críticos. Se realizó el proceso de actualización de los sistemas operativos de los servidores de forma manual en horario nocturno para no afectar la producción de la organización.
- Se realizó la implementación de un WAF en la infraestructura tecnológica de Seguros Alianza S.A. ya que es indispensable para que se puedan solventar las vulnerabilidades que fueron encontradas en los servidores donde se encuentran alojadas las aplicaciones web.

4.5 Evaluación y recomendaciones de los resultados obtenidos

El plan de remediación de vulnerabilidades en la infraestructura tecnológica de Seguros Alianza S.A. ha sido fundamental para identificar y determinar los servidores más críticos. Estos servidores, en su mayoría servidores web, presentan un alto riesgo de sufrir ataques cibernéticos, ya que anteriormente carecían de controles que mitigaran las vulnerabilidades inherentes a las aplicaciones web. Las aplicaciones web son ampliamente utilizadas en la organización para impulsar la mejora continua y la producción del negocio.

Mediante un análisis exhaustivo de cada uno de los servidores identificados como críticos, hemos podido implementar controles y medidas correctivas con el objetivo de reducir el riesgo. Estas acciones buscan salvaguardar la privacidad de los datos personales, así como los datos sensibles de la organización, al mismo tiempo que mejoran la seguridad de las aplicaciones web que se encuentran en producción. Estas aplicaciones web desempeñan un papel fundamental en la gestión, administración y emisión de pólizas de Seguros Alianza S.A.

Al identificar los servidores críticos y realizar un análisis detallado, hemos podido establecer un conjunto de controles y medidas adecuadas para mitigar las vulnerabilidades identificadas. Estas medidas incluyeron con la implementación de firewalls, sistemas de detección de intrusiones, autenticación de dos factores, encriptación de datos, parches de seguridad regulares y otras soluciones tecnológicas avanzadas.

Además de las medidas tecnológicas, también hemos puesto énfasis en la concienciación y capacitación del personal de la organización. La formación en seguridad cibernética y las mejores prácticas de seguridad informática son

fundamentales para fortalecer la postura de seguridad de la organización y prevenir posibles brechas de seguridad.

La implementación de estas medidas correctivas ha permitido reducir significativamente el riesgo asociado a los servidores críticos, garantizando así la confidencialidad, integridad y disponibilidad de la información sensible. Estas acciones contribuyen a fortalecer la seguridad global de la infraestructura tecnológica de Seguros Alianza S.A. y a proteger los activos de información de la organización contra posibles ataques cibernéticos.

5. MATERIALES Y METODOLOGÍA

5.1 Análisis Comparativo de los diferentes WAF disponibles en el Mercado determinando cual es el óptimo para la Implementación en Seguros Alianza S.A.

A partir de esta comparativa, se llevará a cabo un análisis detallado de las características, ventajas y desventajas de cada opción para determinar cuál es la herramienta más indicada para la implementación y configuración del WAF en Seguros Alianza S.A. Este análisis tendrá en cuenta los requisitos específicos de la infraestructura tecnológica de la organización, así como las necesidades de seguridad y las capacidades del equipo de TI.

Se evaluará la funcionalidad, que representa las capacidades y características relacionadas con la protección de aplicaciones web, como la detección de ataques, la prevención de intrusiones y la gestión de políticas de seguridad. Además, se considerará la seguridad Y, que abarca aspectos como la detección y mitigación de vulnerabilidades, la autenticación de usuarios y la protección de datos sensibles.

Asimismo, se analizarán las ventajas y desventajas de cada WAF, tales como su capacidad de escalabilidad, la amplitud de su cobertura de seguridad, la personalización disponible, el precio y la complejidad de configuración. Estos factores serán determinantes para elegir la herramienta que mejor se adapte a las necesidades específicas de Seguros Alianza S.A., brindando un equilibrio óptimo entre funcionalidad, seguridad, costo y facilidad de implementación.

Una vez finalizado el análisis comparativo y la evaluación de las diferentes opciones de WAF, se seleccionará la herramienta más adecuada para llevar a cabo la implementación y configuración en la infraestructura tecnológica de Seguros Alianza S.A. Esta elección se basará en un enfoque estratégico que garantice una protección efectiva de las aplicaciones web contra ataques cibernéticos, salvaguardando así la integridad, confidencialidad y disponibilidad de la información crítica de la organización.

WAF	Descripción	Ventajas	Desventajas
Imperva	Imperva es un servicio de Cortafuegos de aplicaciones web (WAF) que destaca por su seguridad e innovación. Ofrece tanto un servicio WAF tradicional como uno dedicado a la nube.	Es uno de los pocos proveedores de WAF presente en muchos países. Ofrece tanto un servicio WAF tradicional como uno específico para la nube.	La reorganización que está experimentando Imperva podría ir en su desventaja porque, especialmente para la línea de productos SecureSphere, podría haber una reducción en las entregas de los servicios y de las funcionalidades.
Akamai	Las compañías que buscan un servicio en la nube WAF que sostenga aplicaciones web a escala y les asegure la seguridad informática eligen Akamai. El servicio WAF ofrecido por Akamai es Kona Site Defender	Se empeña constantemente en el desarrollo y mejora de las soluciones de seguridad de las aplicaciones web. Las organizaciones que administran diferentes aplicaciones eligen Akamai	Kona Site Defender puede ser elegido solo por clientes que usan servicios en la nube, ya que no existe para los entornos tradicionales.
F5	Es conocido por Big-Ip y Viprion (que pertenecen a la serie ADC). Los productos de seguridad informática son importantes para F5 que ha	Está apostado mucho por los aspectos de seguridad de sus aplicaciones WAF.	Los precios que no son extremadamente competitivos y la falta de productos en su oferta.

	dedicado un área de negocios para desarrollarlos.	El excelente servicio de atención en el cliente y la atestada comunidad de usuarios	La infraestructura de Silverline, el servicio de protección se está quedando atrás respecto a la de sus competidores
Fortinet	La cuota de mercado en el segmento de los dispositivos WAF de Fortinet continúa creciendo gracias a la mejora de las funcionalidades de seguridad	Los productos de Fortinet logran detectar ataques informáticos rápido, también gracias al uso de los algoritmos de aprendizaje automático. Fortinet está aprovechando de la misma estrategia que ha llevado al éxito otros sus productos ofreciendo 8 dispositivos de hardware con una buena relación calidad/precio. Fortinet está invirtiendo mucho en mejorar las funcionalidades de FortiWeb y FortiWeb Cloud.	El retraso de Fortinet en la entrega de los servicios WAF para la nube no fue un buen paso porque FortiWeb Cloud tiene menos funcionalidades que otros productos de los competidores y también tiene menos funcionalidades que FortiWeb [10]

Tabla 18. Comparativa de WAF competitivos en el mercado

Basándonos en la comparación presentada en la tabla 5, se puede concluir que existen diversos tipos de cortafuegos de aplicaciones web (WAF), ya sea de naturaleza comercial o de código abierto, que ofrecen una protección adecuada para las aplicaciones web. Cada una de estas herramientas tiene sus propias características, ventajas y desventajas. En este contexto, se destaca que Fortinet se posiciona como la solución tecnológica que mejor se adapta a las necesidades y requisitos de la organización. Esto se debe a que presenta una serie de ventajas significativas en comparación con sus competidores. Además, es importante mencionar que en Seguros Alianza S.A ya se ha implementado con éxito un dispositivo FortiWeb como firewall de red, lo que hace que la infraestructura tecnológica sea altamente compatible con la implementación de un WAF.

5.2 Detalle de las aplicaciones web que van a ser protegidas

En la tabla 6, se proporciona información detallada sobre las aplicaciones web que se incluirán en la protección del cortafuegos de aplicaciones web (WAF). Se presentan las funcionalidades y particularidades de cada una de estas aplicaciones. Además, para cada aplicación mencionada en la tabla, se presenta un porcentaje de calificación de vulnerabilidades. Estas calificaciones se basan en los criterios que se definieron durante una reunión con el equipo de operaciones del departamento de tecnología de Seguros Alianza S.A.

Aplicación Web	Descripción	Funcionalidad	Sistema Operativo	Lenguaje de Programación	Base de Datos	Arquitectura	Vulnerabilidad por S.O.	Vulnerabilidad por B.D.	Vulnerabilidad por L. P
Incidencias	Permite a los usuarios registrar una solicitud de soporte	Los usuarios tienen acceso al aplicativo para poder solicitar soporte el cual se maneja por tiempos y estados, trabaja mediante correo electrónico notificando tanto al personal de T.I que se encuentra una incidencia registrada como al usuario notificando que su incidencia ya se encuentra resuelta	Microsoft Windows Server Standard 2007	Java (GeneXus)	MySQL	Web	45%	15%	10%
Autoclick	Gestión para la emisión de pólizas	Permite a los usuarios realizar la gestión para la emisión de	Microsoft Windows		DB2	Web	10%	8%	10%

		pólizas, creación de clientes, cotizaciones, consultas, impresión de pólizas, formularios de clientes, autoinspección de vehículos	Server Standard 2012 R2	Java (GeneXus)					
Facturación Electrónica	Gestión para la autorización de documentos electrónicos	Permite a los usuarios verificar y consultar las facturas, notas de crédito, retenciones y liquidaciones de compra, los usuarios administradores pueden realizar la autorización electrónica del RIDE con el SRI	Microsoft Windows Server Standard 2008 R2 Standard	Java (GeneXus)	MySQL	Web	40%	10%	10%
Oficina Virtual	Gestión y consulta de pólizas	Permite a los usuarios dependiendo del rol asignado ingresar para realizar apertura de siniestros consultas y administración de usuarios tiene el acceso para clientes, colaboradores y corredores de seguros	Microsoft Windows Server 2016 Standard	Java (GeneXus)	DB2	Web	15%	10%	10%

Tabla 19. Aplicaciones Web para proteger por el WAF

5.3 Esquema de funcionamiento y seguridad de la infraestructura tecnológica de Seguros Alianza S.A.

El primer aspecto para considerar al desplegar una herramienta de cortafuegos de aplicaciones web (WAF) es la capacidad de establecer políticas de seguridad basadas en diversos criterios, como firmas de ataques conocidos, estándares de protocolo variados y comportamientos anómalos en el tráfico de aplicaciones, entre otros. En este contexto, el enfoque se centra en la evaluación del comportamiento del tráfico web.

De esta manera, cuando el WAF detecta cualquier tipo de infracción, ataque, intento de intrusión o exposición de información confidencial, procede a bloquear el tráfico web. Esto implica la eliminación de solicitudes o respuestas HTTP no autorizadas y evita que tales comportamientos o ataques afecten la integridad de las aplicaciones, garantizando así la seguridad de los datos sensibles. Cuando se detecta una solicitud legítima de acuerdo con la política de seguridad establecida, el WAF permitirá que la solicitud continúe, lo que resultará en una comunicación fluida y segura.

La política de seguridad formulada durante la implementación del WAF también abarca la distinción entre modelos de seguridad positivos y negativos. El modelo positivo permite que únicamente el tráfico predefinido sea autorizado, bloqueando cualquier otro tipo de tráfico. Por otro lado, el modelo negativo se encarga de detectar y bloquear todo el tráfico que se ajusta a patrones definidos como maliciosos.

La figura siguiente representa la referencia a la infraestructura tecnológica y el esquema general propuesto para la implementación del WAF en la organización.

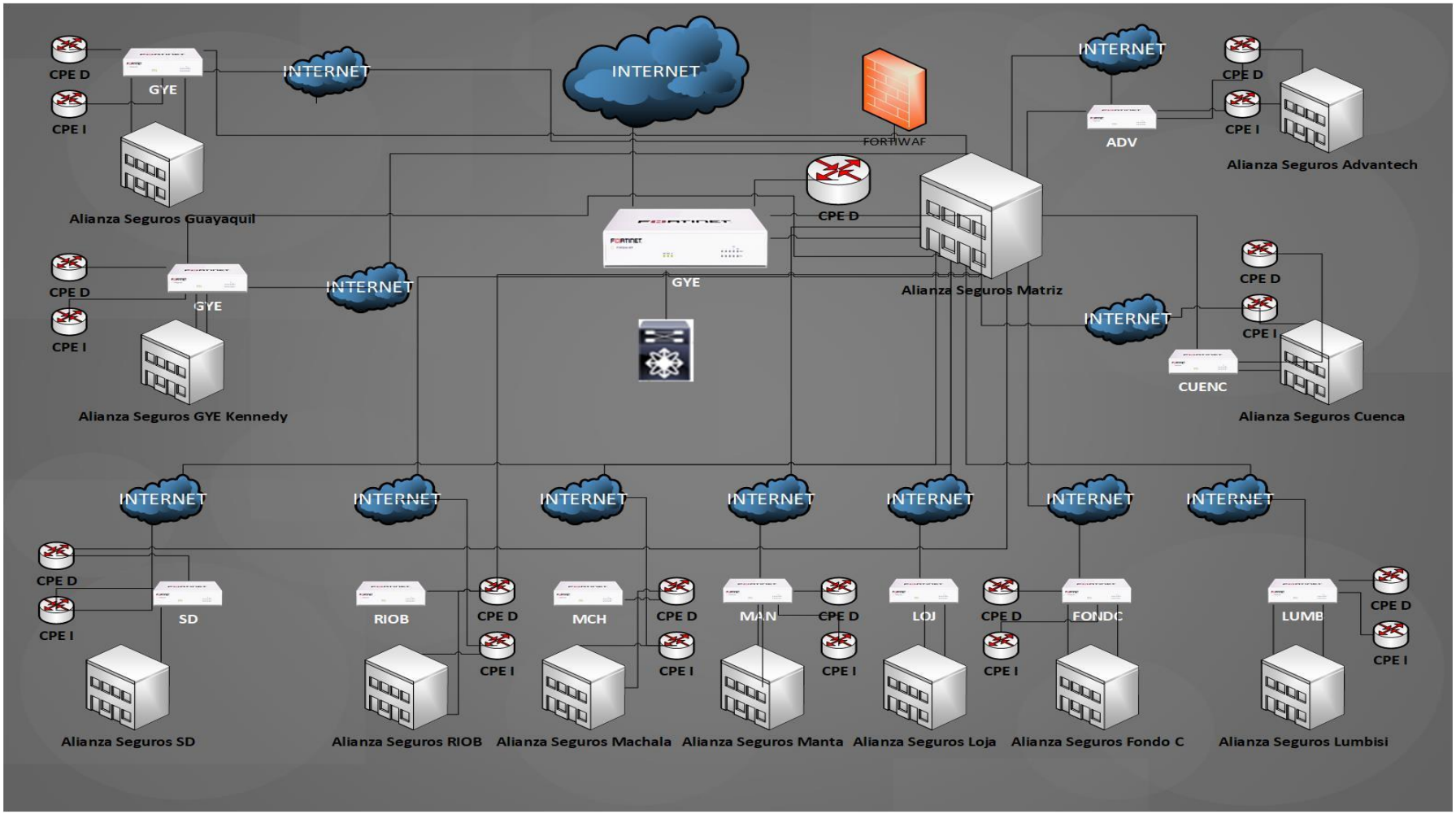


Figura 7. Infraestructura tecnológica propuesta

5.4 Implementación del WAF

Después de completar el proceso de recopilación de información y el levantamiento de datos de la aplicación que requerirá protección mediante el WAF, se procede a detallar los pasos iniciales para configurar el WAF en FortiWeb.

A continuación, se presenta una descripción paso a paso de la configuración del WAF, así como los pasos técnicos necesarios para poner en marcha y configurar cada aplicación web:

Con la implementación y configuración adecuadas del WAF en FortiWeb, Seguros Alianza S.A. podrá garantizar una protección sólida y confiable para sus aplicaciones web, mitigando los riesgos de ataques y asegurando la integridad y seguridad de la infraestructura tecnológica.

Para comenzar, se debe iniciar sesión en la máquina virtual de FortiWeb a través de la pantalla de inicio de sesión en VMware ESXi. Esta interfaz proporciona acceso a la administración y configuración de la máquina virtual.

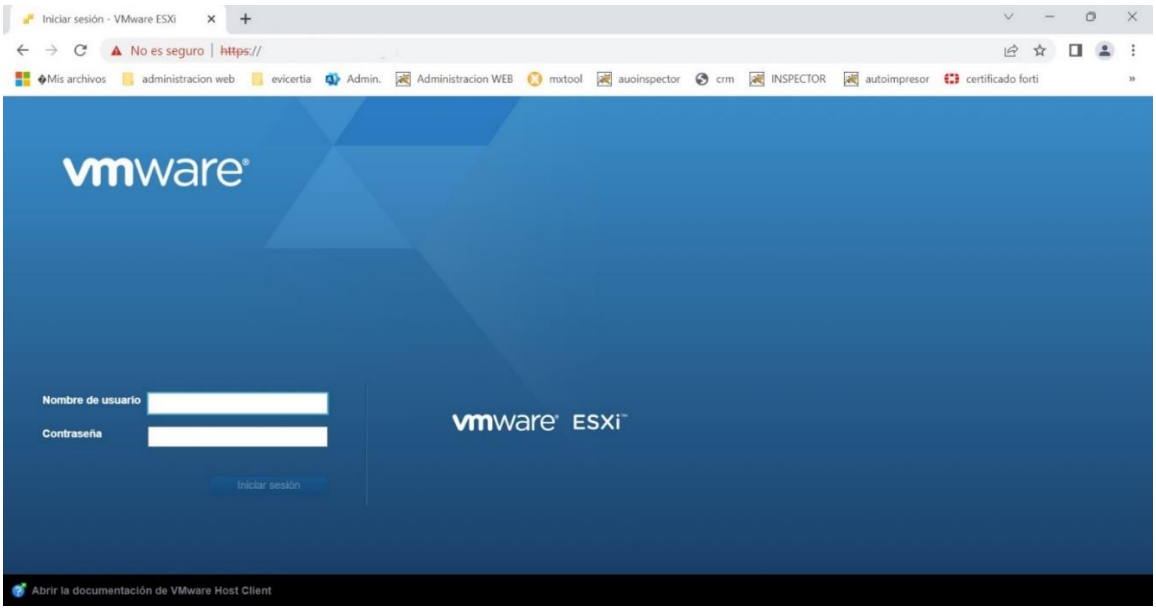


Figura 8. Inicio de sesión en VMware ESXI

Una vez que se ha accedido a la administración de la máquina virtual en la cual se ha configurado FortiWeb para Seguros Alianza S.A., se puede observar las diversas características y funcionalidades que posee esta máquina virtual.

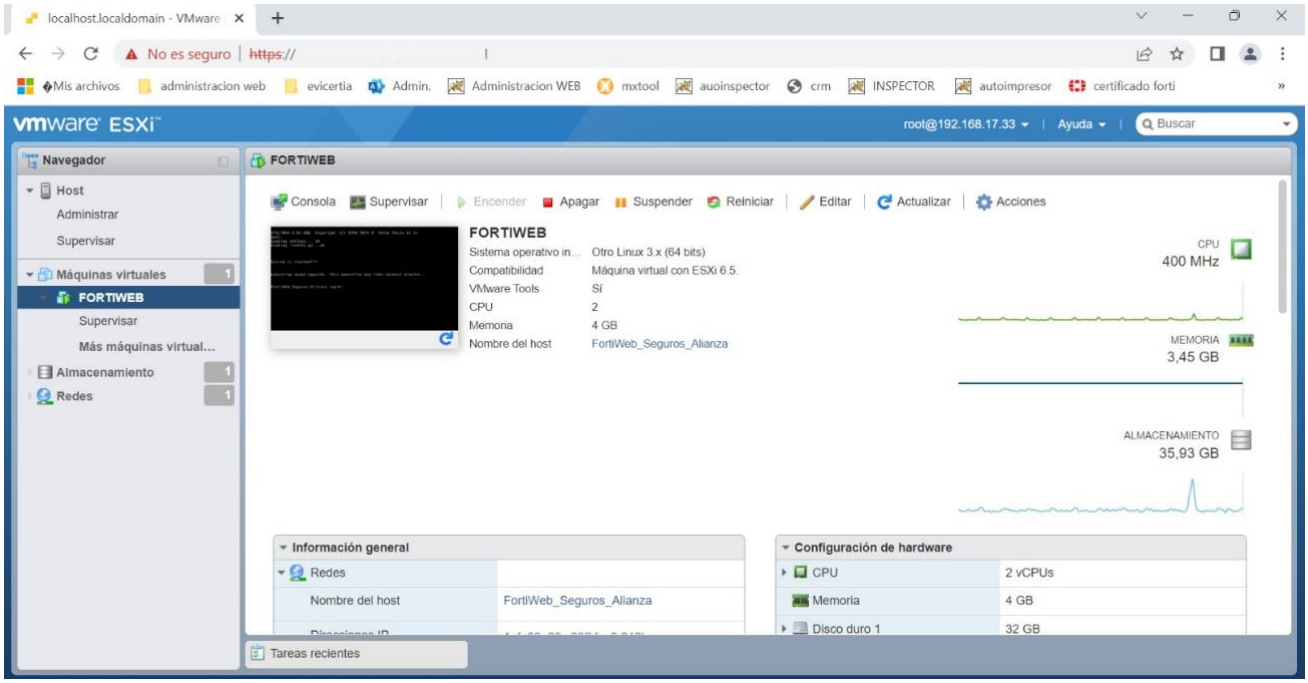


Figura 9. Administración de máquina virtual FortiWeb

En la figura 9, se presenta la información general de la máquina virtual que alberga el sistema FortiWeb, así como las configuraciones relacionadas con las direcciones IP utilizadas en el entorno.

En la sección de información general, se proporciona una visión general de la máquina virtual, incluyendo detalles como el nombre de la máquina, el identificador único, la ubicación física y la versión del sistema operativo utilizado. Estos datos son importantes para identificar y distinguir la máquina virtual específica en el entorno de Seguros Alianza S.A.

En cuanto a las configuraciones de direcciones IP, se muestran los diferentes tipos de direcciones IP asociadas a la máquina virtual. Estas direcciones pueden incluir:

- Dirección IP principal: Es la dirección IP principal asignada a la máquina virtual, que se utiliza como punto de acceso principal para acceder al sistema FortiWeb y gestionar sus configuraciones. Esta dirección IP suele estar conectada a la interfaz de administración y puede ser accesible desde la red interna o desde ubicaciones externas autorizadas.
- Direcciones IP secundarias: Además de la dirección IP principal, la máquina virtual puede tener asignadas direcciones IP secundarias, que se utilizan para diferentes propósitos, como la configuración de interfaces adicionales, la segregación de tráfico o la implementación de servicios específicos. Estas direcciones IP secundarias pueden estar vinculadas a interfaces de red virtuales adicionales en la máquina virtual.

También se puede incluir información adicional sobre las configuraciones de red, como las máscaras de subred asociadas, las puertas de enlace predeterminadas y las políticas de seguridad de red aplicadas.

Estos detalles relacionados con las direcciones IP son fundamentales para garantizar la conectividad y el enrutamiento adecuados en el entorno de Seguros Alianza S.A., así como para permitir el acceso y la administración segura del sistema FortiWeb desde ubicaciones autorizadas.

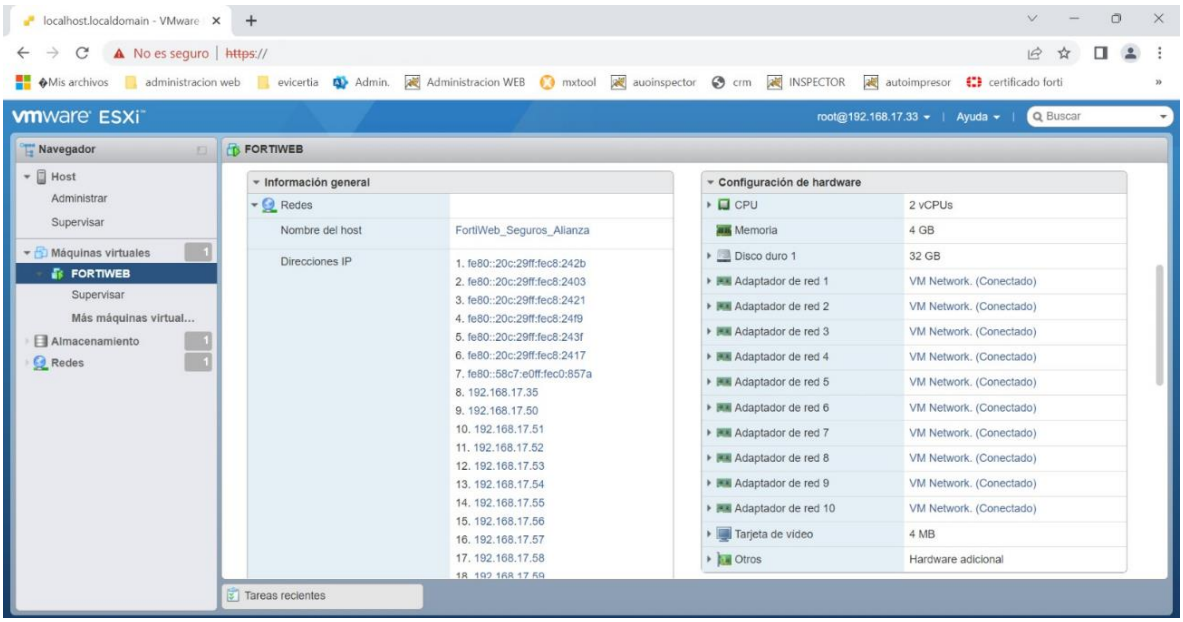


Figura 10. Información general de FortiWeb de Seguros Alianza S.A.

En la figura 10, se muestra la consola de administración del sistema FortiWeb, que es una interfaz gráfica que permite acceder y gestionar todas las funciones y configuraciones del dispositivo de seguridad.

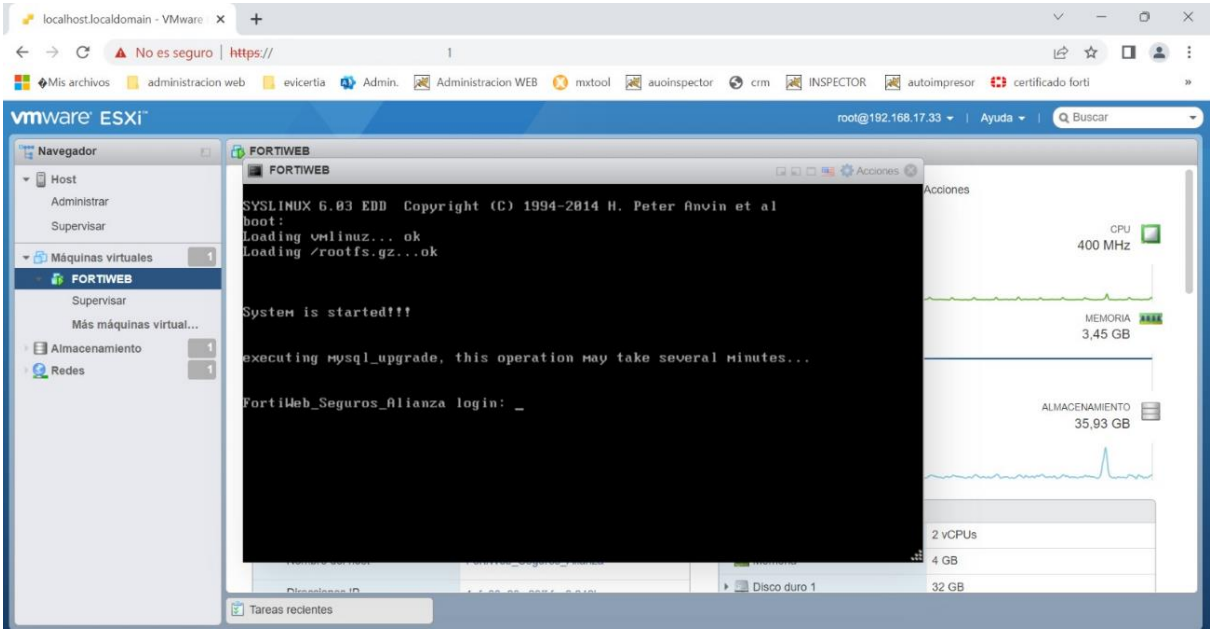


Figura 11. Consola de administración de FortiWeb

La consola del FortiWeb proporciona una vista centralizada y fácil de usar para administrar y monitorear las políticas de seguridad, las reglas de filtrado, las listas de control de acceso y otros aspectos relacionados con la protección de las aplicaciones web. Esta interfaz de administración permite a los administradores configurar y personalizar los ajustes del WAF de acuerdo con los requisitos específicos de Seguros Alianza S.A.

Al ingresar a la consola del FortiWeb, los administradores tienen acceso a diferentes secciones y paneles que brindan información y opciones de configuración.

La consola del FortiWeb es una herramienta fundamental para la administración y configuración de las políticas de seguridad aplicadas a las aplicaciones web protegidas. A través de esta interfaz, los administradores pueden mantener un control preciso sobre la seguridad de las aplicaciones, detectar y prevenir ataques cibernéticos, y garantizar la disponibilidad y la integridad de los servicios web en el entorno de Seguros Alianza S.A.

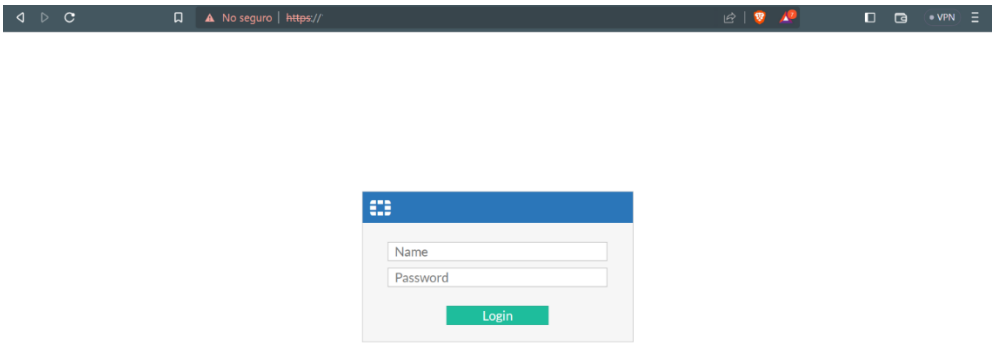


Figura 12. Inicio de sesión a FortiWeb

En la figura 12, se muestra la pantalla de inicio de sesión del sistema FortiWeb, que es la interfaz de autenticación que permite a los usuarios autorizados acceder y administrar las configuraciones y funciones del WAF.

El inicio de sesión en FortiWeb es un paso crucial para garantizar la seguridad y el acceso controlado a las funciones de administración. Los usuarios autorizados deben ingresar sus credenciales, que generalmente consisten en un nombre de usuario y una contraseña, para autenticarse y obtener acceso a la consola de administración.

La pantalla de inicio de sesión proporciona un campo para ingresar el nombre de usuario y otro campo para ingresar la contraseña correspondiente. Los usuarios deben proporcionar la información de autenticación correcta para que el sistema FortiWeb pueda verificar su identidad y otorgarles los privilegios y permisos adecuados.

Es importante resaltar que el inicio de sesión en FortiWeb debe llevarse a cabo por usuarios autorizados y con las credenciales adecuadas para garantizar la seguridad del sistema y prevenir accesos no autorizados.

Una vez que los usuarios han completado el inicio de sesión de manera exitosa, se le concederá acceso a la consola de administración del FortiWeb, donde podrán

configurar y administrar las políticas de seguridad, supervisar el tráfico de aplicaciones web, revisar registros de eventos, generar informes y realizar otras tareas relacionadas con la protección y gestión de las aplicaciones web.

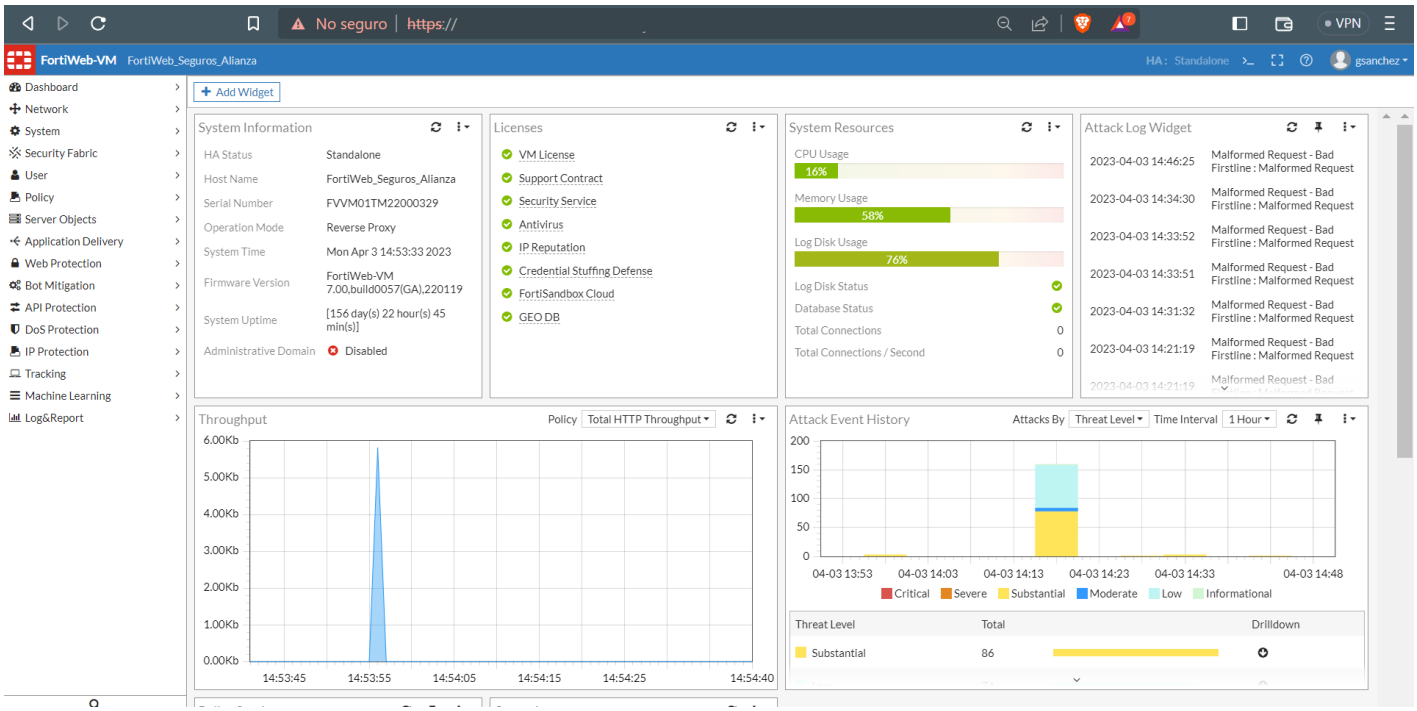


Figura 13. Entorno de FortiWeb

En la figura 13, se presenta la interfaz y la pantalla principal del cortafuegos de aplicaciones web (WAF), donde se despliegan diversas opciones y características que permiten llevar a cabo las configuraciones de seguridad necesarias para proteger las aplicaciones web.

La pantalla principal del WAF muestra una visión general del sistema, brindando información estadística relevante sobre el rendimiento y el estado del sistema. Esto incluye detalles como la carga de CPU, el consumo de memoria, el tráfico de red y otros recursos del sistema. Estos datos son importantes para monitorear y garantizar un funcionamiento óptimo del WAF.

Además, en esta pantalla se muestran las licencias asociadas al WAF, lo que permite verificar su validez y disponibilidad. Las licencias son esenciales para acceder a todas las funcionalidades y características del WAF, por lo que es importante contar con ellas de manera adecuada.

El entorno del WAF en la figura 12 también presenta opciones para acceder a diferentes vistas e informes relacionados con la seguridad. Por ejemplo, se pueden visualizar los logs de ataques, que registran los intentos de intrusión o actividades maliciosas dirigidas a las aplicaciones web protegidas por el WAF. Estos logs son valiosos para identificar y analizar los patrones de ataque, así como para tomar medidas correctivas.

Asimismo, se ofrecen diversas opciones de configuración de seguridad en esta interfaz principal del WAF. Estas opciones permiten establecer políticas de seguridad personalizadas, configurar reglas de filtrado, habilitar o deshabilitar funciones específicas del WAF y adaptar la protección a las necesidades particulares de las aplicaciones web y de la organización.

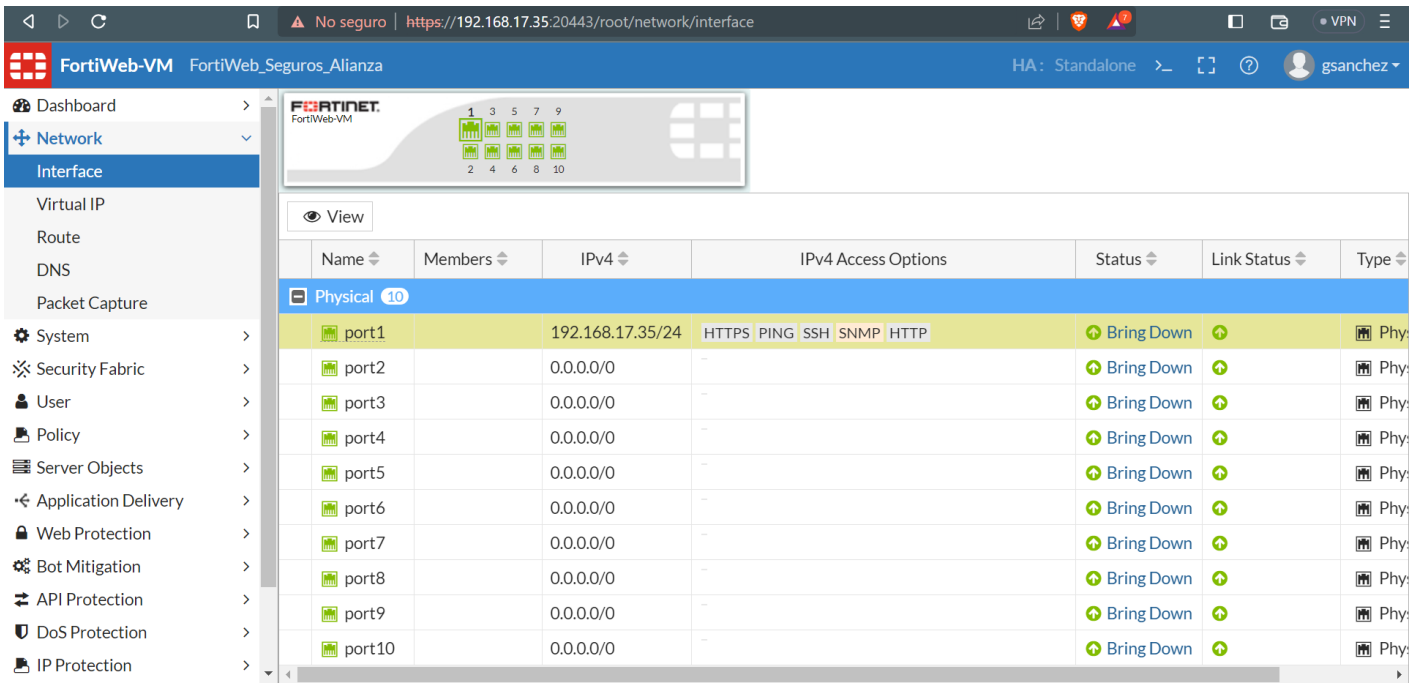


Figura 14. Interfaz de red

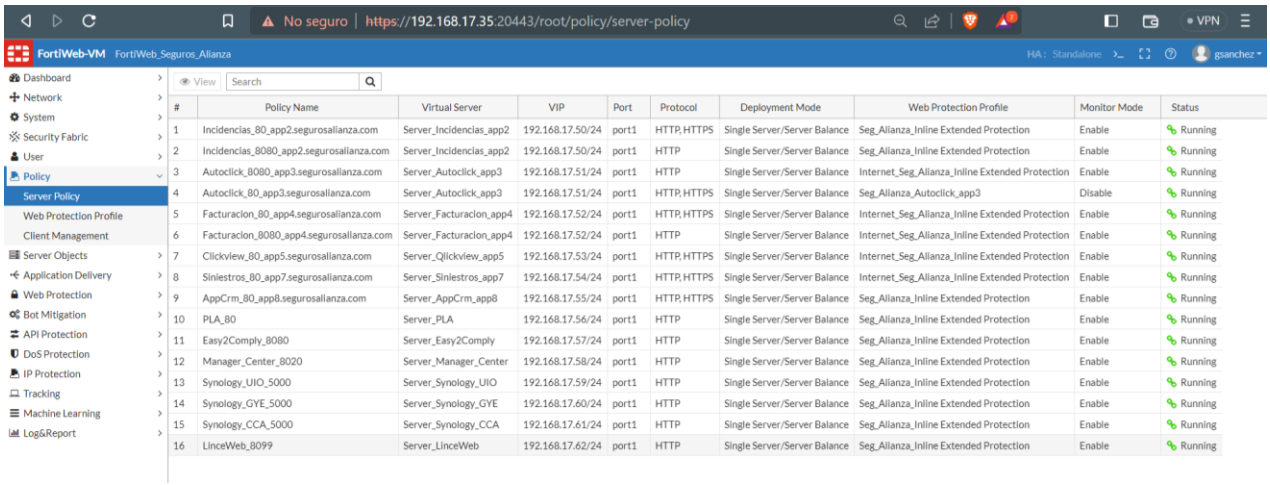
En la figura 14, se presenta el puerto 1 de la interfaz de red del cortafuegos de aplicaciones web (WAF). Este puerto representa la conexión física a través de la cual el WAF se conecta a la red para recibir y enviar tráfico de datos.

La configuración de la interfaz de red es un aspecto crucial en el despliegue del WAF, ya que determina cómo se establecerá la comunicación con otras máquinas y dispositivos en la red. En este caso, el puerto 1 corresponde a una interfaz específica del WAF que se ha configurado para interactuar con la red.

En la figura 13, se pueden observar diferentes parámetros y configuraciones relacionadas con el puerto 1. Esto puede incluir detalles como la dirección IP asignada a este puerto, la máscara de subred correspondiente, la velocidad de transmisión de datos, el estado de la interfaz (activada o desactivada) y otras opciones de configuración específicas de red.

Es importante destacar que el puerto 1 puede representar una de las múltiples interfaces de red disponibles en el WAF. Dependiendo de la arquitectura y los requisitos de la infraestructura, es posible que se utilicen varios puertos para establecer conexiones con distintas redes o segmentos de red.

La configuración adecuada de la interfaz de red garantiza que el WAF pueda recibir el tráfico de datos entrante y saliente de manera eficiente y segura. Además, permite establecer reglas de filtrado y aplicar políticas de seguridad en función de las comunicaciones que se produzcan a través de este puerto.



#	Policy Name	Virtual Server	VIP	Port	Protocol	Deployment Mode	Web Protection Profile	Monitor Mode	Status
1	Incidencias_80_app2.segurosalianza.com	Server_Incidencias_app2	192.168.17.50/24	port1	HTTP, HTTPS	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
2	Incidencias_8080_app2.segurosalianza.com	Server_Incidencias_app2	192.168.17.50/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
3	Autoclick_8080_app3.segurosalianza.com	Server_Autoclick_app3	192.168.17.51/24	port1	HTTP	Single Server/Server Balance	Internet_Seg_Alianza_Inline Extended Protection	Enable	Running
4	Autoclick_80_app3.segurosalianza.com	Server_Autoclick_app3	192.168.17.51/24	port1	HTTP, HTTPS	Single Server/Server Balance	Seg_Alianza_Autoclick_app3	Disable	Running
5	Facturacion_80_app4.segurosalianza.com	Server_Facturacion_app4	192.168.17.52/24	port1	HTTP, HTTPS	Single Server/Server Balance	Internet_Seg_Alianza_Inline Extended Protection	Enable	Running
6	Facturacion_8080_app4.segurosalianza.com	Server_Facturacion_app4	192.168.17.52/24	port1	HTTP	Single Server/Server Balance	Internet_Seg_Alianza_Inline Extended Protection	Enable	Running
7	Clickview_80_app5.segurosalianza.com	Server_Qlickview_app5	192.168.17.53/24	port1	HTTP, HTTPS	Single Server/Server Balance	Internet_Seg_Alianza_Inline Extended Protection	Enable	Running
8	Siniestros_80_app7.segurosalianza.com	Server_Siniestros_app7	192.168.17.54/24	port1	HTTP, HTTPS	Single Server/Server Balance	Internet_Seg_Alianza_Inline Extended Protection	Enable	Running
9	AppCrm_80_app8.segurosalianza.com	Server_AppCrm_app8	192.168.17.55/24	port1	HTTP, HTTPS	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
10	PLA_80	Server_PLA	192.168.17.56/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
11	Easy2Comply_8080	Server_Easy2Comply	192.168.17.57/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
12	Manager_Center_8020	Server_Manager_Center	192.168.17.58/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
13	Synology_UIO_5000	Server_Synology_UIO	192.168.17.59/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
14	Synology_GYE_5000	Server_Synology_GYE	192.168.17.60/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
15	Synology_CCA_5000	Server_Synology_CCA	192.168.17.61/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running
16	LinceWeb_8099	Server_LinceWeb	192.168.17.62/24	port1	HTTP	Single Server/Server Balance	Seg_Alianza_Inline Extended Protection	Enable	Running

Figura 15. Políticas del servidor

En la figura 15, se presenta la interfaz que muestra las políticas del servidor del cortafuegos de aplicaciones web (WAF). Estas políticas son configuraciones específicas que se establecen para proteger las aplicaciones web y gestionar el tráfico de datos que fluye a través del WAF.

En esta figura, se pueden observar las diferentes políticas implementadas, las cuales están diseñadas para vincular las URL de las aplicaciones web con las IP virtuales asignadas. Esto permite establecer reglas de seguridad y aplicar medidas de protección personalizadas para cada aplicación.

La relación entre las URL y las IP virtuales es fundamental para garantizar que el tráfico de datos se dirija correctamente hacia las aplicaciones web específicas y que se apliquen las medidas de seguridad adecuadas. Al establecer estas políticas, se pueden configurar acciones específicas, como la inspección de paquetes, el filtrado de contenido, la detección de intrusos y la prevención de ataques, entre otras.

La configuración de políticas del servidor en el WAF implica definir reglas y acciones para diferentes escenarios y tipos de tráfico. Esto puede incluir permitir o bloquear el acceso a ciertas URL, aplicar protección contra ataques conocidos, configurar listas de control de acceso (ACL) y definir políticas de seguridad personalizadas según los requisitos de cada aplicación web.

Además de las URL y las IP virtuales, la interfaz de políticas del servidor puede mostrar otros parámetros y configuraciones relevantes. Esto puede incluir opciones de enrutamiento, configuraciones de equilibrio de carga, reglas de redireccionamiento y otras funcionalidades avanzadas que permiten optimizar el rendimiento y la seguridad de las aplicaciones web protegidas.

En resumen, la figura 15 muestra la interfaz de políticas del servidor en el WAF, donde se establecen las configuraciones relacionadas con las URL de las aplicaciones web y las IP virtuales. Estas políticas permiten implementar medidas de seguridad personalizadas y dirigir el tráfico de datos hacia las aplicaciones web de manera segura y eficiente.

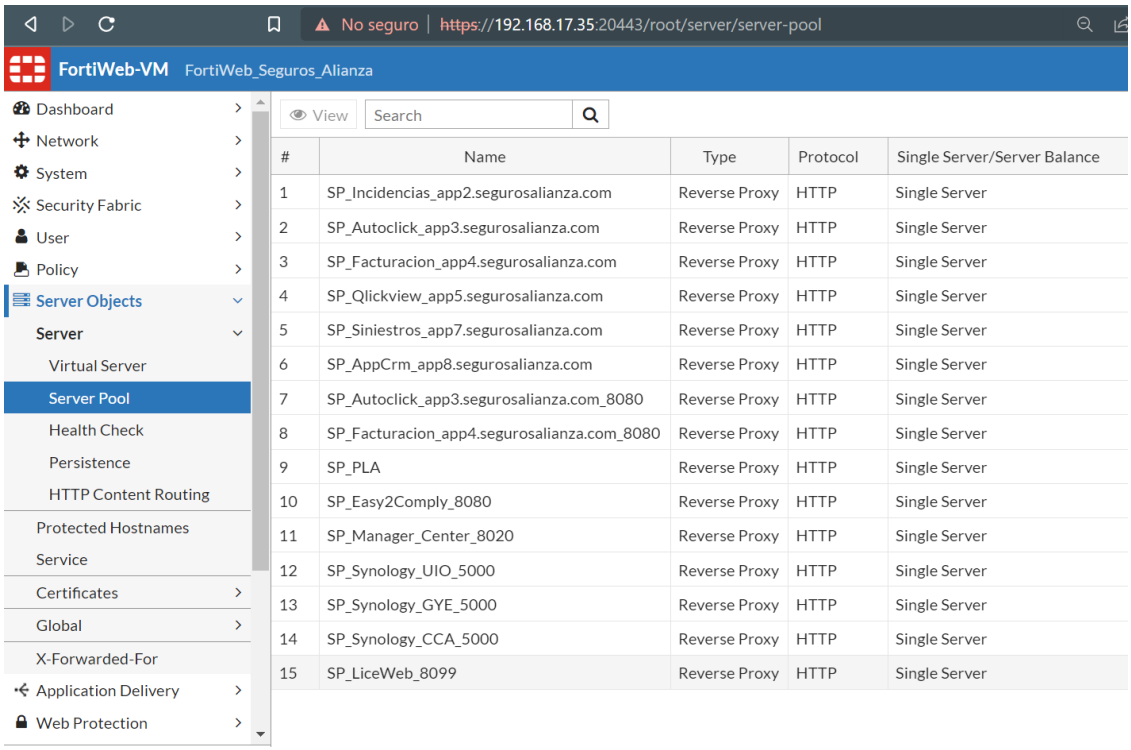


Figura 16. Grupo de servidores

En la figura 16, se presenta la interfaz de configuración del grupo de servidores en el entorno del cortafuegos de aplicaciones web (WAF). En este contexto, un grupo de servidores se refiere a un conjunto de aplicaciones web que se encuentran configuradas en modo de proxy inverso.

El proxy inverso es una configuración en la que el WAF actúa como intermediario entre los clientes y los servidores de aplicaciones web. Esto implica que todas las

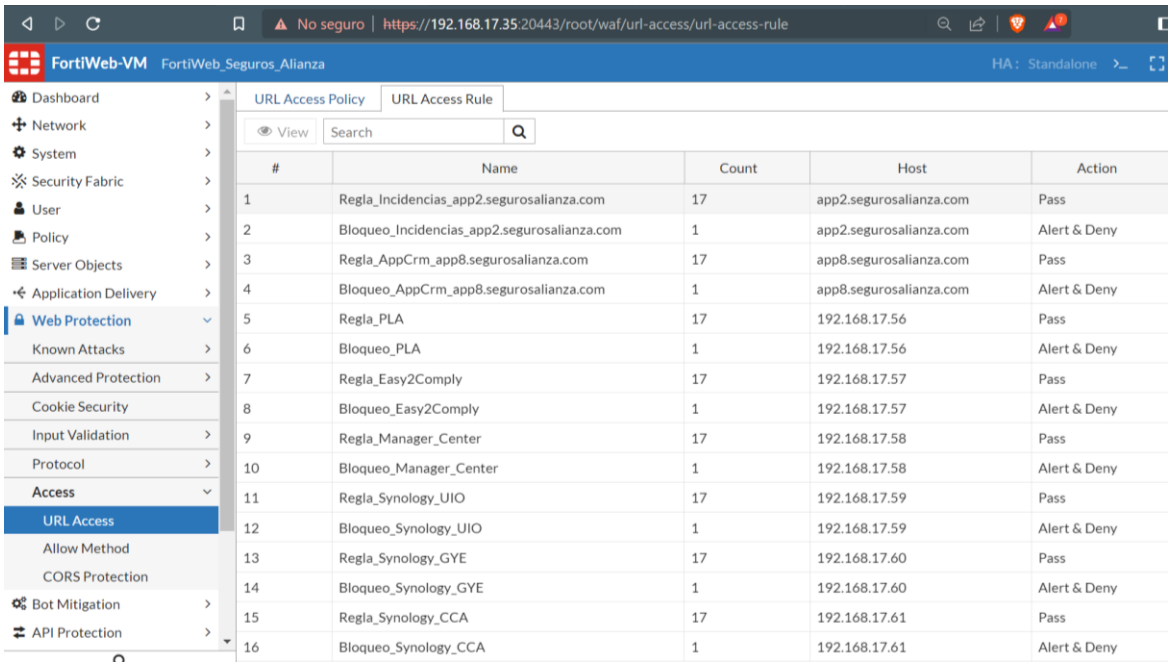
solicitudes de los clientes pasan a través del WAF antes de ser enviadas a los servidores de aplicaciones correspondientes. El WAF analiza y filtra el tráfico entrante y saliente para aplicar medidas de seguridad y protección.

En la figura 16, se pueden observar las diferentes aplicaciones web que se han configurado dentro del grupo de servidores. Estas aplicaciones web pueden representar diferentes servicios o funciones dentro de la organización, y se les asigna una configuración específica en términos de reglas de seguridad, políticas de acceso y acciones de protección.

Al establecer el grupo de servidores en modo reverse proxy, el WAF se encarga de enrutar las solicitudes de los clientes a las aplicaciones web correspondientes según la configuración definida. Esto proporciona una capa adicional de seguridad al ocultar la infraestructura de servidores de aplicaciones detrás del WAF y controlar el flujo de tráfico de manera centralizada.

La configuración del grupo de servidores en modo reverse proxy implica establecer reglas de enrutamiento, configurar puertos y direcciones IP, definir políticas de acceso y establecer acciones de protección específicas para cada aplicación web. Esto permite gestionar el tráfico de manera eficiente, proteger las aplicaciones web de posibles ataques y garantizar un acceso seguro y controlado por parte de los usuarios.

Además de las configuraciones mencionadas, la interfaz de configuración del grupo de servidores puede mostrar otros parámetros y opciones avanzadas, como configuraciones de balanceo de carga, reglas de redireccionamiento, configuraciones de caché y otras funcionalidades que permiten optimizar el rendimiento y la seguridad de las aplicaciones web en el entorno del WAF.



#	Name	Count	Host	Action
1	Regla_Incidencias_app2.segurosalianza.com	17	app2.segurosalianza.com	Pass
2	Bloqueo_Incidencias_app2.segurosalianza.com	1	app2.segurosalianza.com	Alert & Deny
3	Regla_AppCrm_app8.segurosalianza.com	17	app8.segurosalianza.com	Pass
4	Bloqueo_AppCrm_app8.segurosalianza.com	1	app8.segurosalianza.com	Alert & Deny
5	Regla_PLA	17	192.168.17.56	Pass
6	Bloqueo_PLA	1	192.168.17.56	Alert & Deny
7	Regla_Easy2Comply	17	192.168.17.57	Pass
8	Bloqueo_Easy2Comply	1	192.168.17.57	Alert & Deny
9	Regla_Manager_Center	17	192.168.17.58	Pass
10	Bloqueo_Manager_Center	1	192.168.17.58	Alert & Deny
11	Regla_Synology_UIO	17	192.168.17.59	Pass
12	Bloqueo_Synology_UIO	1	192.168.17.59	Alert & Deny
13	Regla_Synology_GYE	17	192.168.17.60	Pass
14	Bloqueo_Synology_GYE	1	192.168.17.60	Alert & Deny
15	Regla_Synology_CCA	17	192.168.17.61	Pass
16	Bloqueo_Synology_CCA	1	192.168.17.61	Alert & Deny

Figura 17. Reglas y bloqueos

En la figura 17, se presenta la interfaz de configuración de reglas y bloqueos dentro del entorno del cortafuegos de aplicaciones web (WAF). Esta sección es de vital importancia para garantizar la seguridad y protección de las aplicaciones web específicas que se encuentran protegidas por el WAF.

En esta vista, se pueden observar todas las reglas y bloqueos que se han configurado para cada una de las aplicaciones web. Estas reglas y bloqueos son medidas de seguridad específicas que se aplican para prevenir y mitigar posibles ataques y vulnerabilidades en las aplicaciones.

Las reglas son instrucciones específicas que definen cómo el WAF debe procesar y filtrar el tráfico de datos que ingresa a las aplicaciones web. Estas reglas pueden incluir la detección y bloqueo de patrones de ataque conocidos, como inyecciones de código SQL, intentos de acceso no autorizado, ataques de fuerza bruta, entre otros.

Por otro lado, los bloqueos son acciones preventivas que se aplican cuando se detecta una actividad sospechosa o maliciosa en una aplicación web. Estos bloqueos pueden implicar la prohibición de direcciones IP o rangos de IP específicos, la negación de

ciertos tipos de solicitudes, la restricción de acciones específicas, entre otras medidas de seguridad.

La configuración de reglas y bloqueos es altamente personalizable y depende de las necesidades y características específicas de cada aplicación web. En la figura 16, se pueden visualizar las reglas y bloqueos establecidos para cada aplicación web protegida por el WAF, lo que proporciona una visión general de las medidas de seguridad implementadas.

Es importante destacar que la configuración de reglas y bloqueos dentro del WAF es un proceso continuo y dinámico. Se requiere un monitoreo constante y una actualización regular de las reglas y bloqueos para adaptarse a las nuevas amenazas y vulnerabilidades que puedan surgir en el entorno de seguridad cibernética.

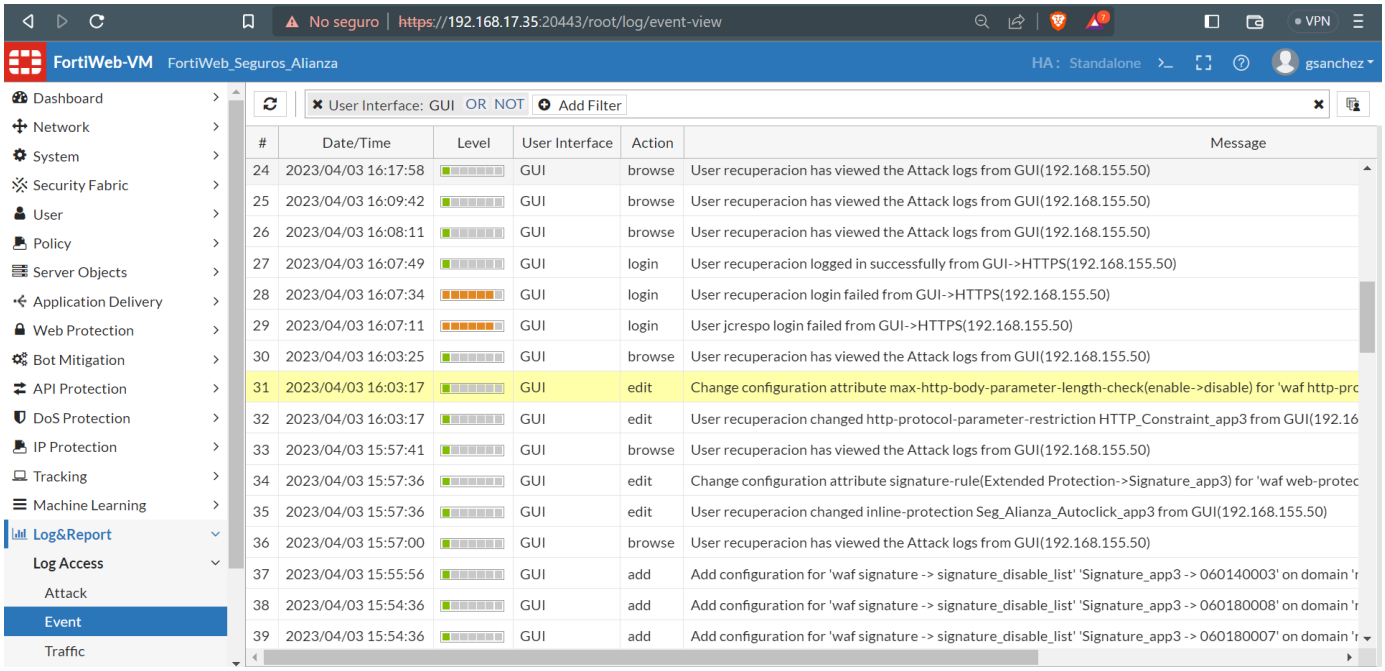


Figura 18. Logs de eventos

En la figura 18, se presenta la vista de los logs de eventos del cortafuegos de aplicaciones web (WAF). Estos logs contienen información detallada sobre los eventos y actividades que el WAF ha detectado y registrado mientras monitorea el tráfico de la aplicación web protegida.

En esta modalidad de escucha, el WAF está constantemente capturando y registrando el tráfico y las acciones que se llevan a cabo en la aplicación web. Esto incluye solicitudes de acceso, interacciones de usuarios, intentos de ataque, respuestas del servidor, entre otros eventos relevantes.

Los logs de eventos proporcionan una valiosa fuente de información para el análisis de seguridad y la detección de posibles amenazas. Estos registros permiten identificar patrones de comportamiento sospechosos, identificar intentos de ataques, analizar el impacto de eventos específicos en la seguridad de la aplicación y realizar investigaciones forenses en caso de incidentes de seguridad.

Los logs suelen contener detalles como la dirección IP del cliente, la URL de la solicitud, el tipo de acción realizada, el código de respuesta del servidor, la fecha y hora del evento, entre otros datos relevantes. Estos registros se organizan de manera cronológica para facilitar el análisis y la comprensión de los eventos ocurridos.

El análisis de los logs de eventos del WAF es una tarea crucial para garantizar la seguridad de la aplicación web y la detección oportuna de posibles amenazas. Esto implica revisar regularmente los registros, aplicar filtros y correlacionar los eventos para identificar patrones o anomalías que requieran una atención especial.

Además, los logs de eventos también se utilizan para generar informes de seguridad, realizar auditorías y cumplir con los requisitos de cumplimiento normativo. Estos informes proporcionan una visión general de la actividad del WAF, destacando los eventos relevantes, las tendencias de seguridad y las métricas clave para evaluar la eficacia de las medidas de protección implementadas.

En resumen, la figura 18 muestra la interfaz de visualización de los logs de eventos del WAF, que registra y muestra información detallada sobre el tráfico y las acciones realizadas en la aplicación web protegida. Estos logs son una herramienta esencial para el monitoreo de la seguridad, la detección de amenazas y el cumplimiento normativo en el entorno de protección del WAF.

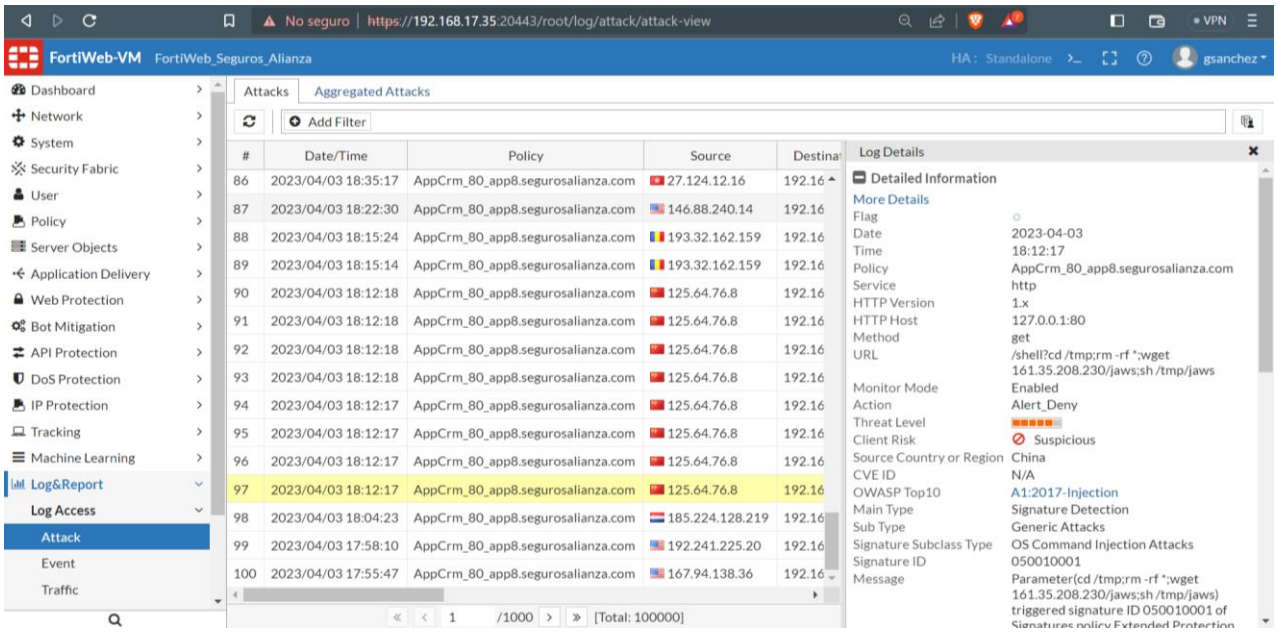


Figura 19. Logs de ataques

En la figura 19, se presenta el log de ataques del cortafuegos de aplicaciones web (WAF). Este log registra y muestra las actividades sospechosas que el WAF ha identificado como posibles ataques a la aplicación web protegida.

El WAF analiza el tráfico entrante y saliente de la aplicación web en busca de patrones y comportamientos maliciosos. Cuando detecta una actividad que coincide con las reglas de detección de ataques configuradas, registra esa actividad en el log de ataques.

Es importante tener en cuenta que, aunque el WAF está diseñado para identificar y bloquear ataques, también existe la posibilidad de falsos positivos. Estos son eventos registrados como ataques por el WAF, pero que en realidad pueden ser solicitudes legítimas o comportamientos no maliciosos.

Para garantizar la eficacia del WAF y minimizar los falsos positivos, es necesario validar y revisar regularmente el log de ataques. Esto implica analizar las actividades registradas, revisar las reglas de detección de ataques y evaluar si las acciones identificadas son realmente amenazas legítimas.

En caso de identificar falsos positivos, es necesario ajustar la configuración del WAF para que realice excepciones y evite bloquear actividades legítimas. Esto puede implicar ajustar las reglas de detección de ataques, modificar los umbrales de sensibilidad o crear excepciones personalizadas para ciertos patrones de tráfico.

La revisión y validación regular del log de ataques es fundamental para mantener un equilibrio adecuado entre la protección contra ataques y la garantía de que las actividades legítimas no se vean afectadas. Esto ayuda a evitar bloqueos innecesarios y asegura que la aplicación web funcione correctamente para los usuarios autorizados.

Además, el análisis del log de ataques puede proporcionar información valiosa sobre las tendencias de ataques, las técnicas utilizadas por los atacantes y los posibles puntos débiles en la aplicación web. Esta información se puede utilizar para fortalecer aún más las medidas de seguridad y realizar mejoras continuas en la protección de la aplicación.

En resumen, la figura 19 muestra el log de ataques del WAF, que registra las actividades sospechosas consideradas como ataques a la aplicación web protegida. La revisión y validación regular de este log es esencial para identificar falsos positivos y ajustar la configuración del WAF en consecuencia, garantizando una protección efectiva contra amenazas legítimas y un funcionamiento óptimo de la aplicación web.

6. Resultados y discusión

Durante la ejecución e implementación del cortafuegos de aplicaciones web (WAF) en la infraestructura tecnológica de Seguros Alianza S.A., se siguieron los procesos de seguridad de la información y ciberseguridad establecidos en la organización. Esta implementación resultó ser de gran importancia, ya que permitió mejorar significativamente la seguridad de las aplicaciones web, las cuales desempeñan un papel crucial en la productividad y funcionamiento corporativo.

La implementación del WAF fue un proceso cuidadoso que implicó la configuración y personalización del sistema de acuerdo con las necesidades y características específicas de las aplicaciones web de la organización. Se establecieron reglas y políticas de seguridad, se llevaron a cabo pruebas exhaustivas y se realizaron ajustes y depuraciones para garantizar una protección óptima en tiempo real.

La incorporación del WAF en la infraestructura tecnológica permitió reducir significativamente el riesgo de sufrir ataques cibernéticos por parte de ciberdelincuentes. El WAF actúa como una barrera de defensa que monitorea y filtra el tráfico de las aplicaciones web, detectando y bloqueando posibles amenazas y ataques maliciosos. Esto brinda una capa adicional de seguridad que complementa otras medidas de protección implementadas en la organización.

Durante todo el proceso de implementación, se realizó un seguimiento continuo de las configuraciones del WAF y se llevaron a cabo pruebas rigurosas para evaluar su eficacia. Se realizaron ajustes y refinamientos en las reglas de seguridad en función del comportamiento y uso de las aplicaciones web, garantizando que el WAF se adapte de manera óptima a las necesidades específicas de Seguros Alianza S.A.

Los resultados obtenidos de la implementación del WAF fueron altamente positivos. Se logró una mejora significativa en la seguridad de las aplicaciones web, disminuyendo la exposición a posibles vulnerabilidades y ataques. La detección temprana y el bloqueo de actividades sospechosas y maliciosas permitieron prevenir

potenciales amenazas y proteger la integridad y confidencialidad de los datos de la organización y de los usuarios.

La implementación del WAF también contribuyó a fortalecer los procesos de seguridad de la información y ciberseguridad en Seguros Alianza S.A. Se establecieron mejores prácticas y se promovió una cultura de seguridad, concientizando a los usuarios y personal técnico sobre la importancia de proteger las aplicaciones web y mantener una postura defensiva frente a las posibles amenazas.

En conclusión, la implementación del WAF en la infraestructura tecnológica de Seguros Alianza S.A. brindó una protección efectiva y mejorada para las aplicaciones web, reduciendo el riesgo de ataques cibernéticos y fortaleciendo los procesos de seguridad de la información. Esta iniciativa representó un paso importante en la gestión integral de la seguridad cibernética de la organización.

6.1 Monitoreo de los Resultados

La implementación de FortiWeb ha permitido establecer un monitoreo continuo para evaluar y analizar los resultados obtenidos. Este monitoreo es de vital importancia, ya que nos brinda la capacidad de identificar patrones y tendencias en el tráfico de las aplicaciones web protegidas, lo que a su vez nos permite definir reglas e indicadores de seguridad más precisos.

El monitoreo constante nos proporciona una visibilidad detallada de las actividades y eventos que ocurren en el entorno protegido por FortiWeb. Mediante la recopilación y análisis de los registros de eventos, podemos detectar posibles amenazas, anomalías o comportamientos sospechosos que podrían indicar intentos de intrusión o ataques cibernéticos.

Con base en los resultados del monitoreo, podemos ajustar y afinar los parámetros de ejecución de FortiWeb. Esto implica realizar modificaciones en las reglas de seguridad, configurar nuevas políticas o adaptar las existentes para adaptarse a las

necesidades y características cambiantes de las aplicaciones web y los posibles ataques que puedan surgir.

Además, el monitoreo nos permite evaluar el rendimiento y la eficacia del WAF en tiempo real. Podemos medir el impacto de las reglas de seguridad implementadas, determinar el nivel de detección y bloqueo de amenazas, evaluar la capacidad de respuesta y la efectividad de las contramedidas aplicadas.

Al establecer un monitoreo adecuado, podemos generar informes periódicos y estadísticas relevantes que nos brindarán una visión más amplia de la seguridad de las aplicaciones web y nos permitirán tomar decisiones informadas. Podremos identificar áreas de mejora, implementar medidas correctivas y fortalecer la postura de seguridad de la organización de manera proactiva.

En resumen, el establecimiento de un monitoreo continuo y exhaustivo nos proporciona la capacidad de evaluar y ajustar de manera efectiva los parámetros de ejecución de FortiWeb. Esto nos ayuda a mantener un nivel óptimo de protección, identificar amenazas potenciales y fortalecer la seguridad de las aplicaciones web en Seguros Alianza S.A. mediante la implementación de reglas de seguridad precisas y la adopción de contramedidas adecuadas.

6.2 Utilización de los Resultados

La ejecución continua del WAF implementado y los resultados obtenidos brindan una valiosa información que permite perfeccionar las técnicas y estrategias de seguridad de la información y ciberseguridad en la organización.

Basándonos en los resultados obtenidos, las personas responsables de la ciberseguridad en la organización pueden tomar decisiones fundamentadas y realizar ajustes necesarios en el programa de seguridad establecido. Estos ajustes pueden incluir actualizaciones o modificaciones de las políticas de seguridad de la información en el departamento de tecnología, con el objetivo de adaptarse a las amenazas y desafíos actuales.

Además, los resultados del WAF también pueden influir en la mejora o modificación de la configuración de la herramienta de monitoreo y seguridad en sí misma. Esto implica revisar y ajustar los parámetros de detección, bloqueo y respuesta del WAF, así como aprovechar las funcionalidades y características avanzadas que ofrece para una protección óptima.

El análisis de los resultados puede revelar áreas de mejora en cuanto a la eficacia de las políticas de seguridad implementadas, la detección y mitigación de amenazas, y la capacidad de respuesta ante incidentes. Estos hallazgos pueden impulsar la implementación de medidas correctivas y mejoras adicionales en la infraestructura tecnológica y los procesos de seguridad.

En resumen, los resultados obtenidos a través de la ejecución y monitoreo continuo del WAF proporcionan una base sólida para actualizar y mejorar el programa de seguridad, las políticas de seguridad de la información y la configuración de la herramienta de seguridad. Estas acciones permiten a la organización mantenerse actualizada y adaptada a las amenazas cibernéticas en constante evolución, fortaleciendo así su postura de seguridad y protegiendo los activos de información de manera efectiva.

6.3 Mejora continua

En esta fase, es fundamental considerar las mejoras que se pueden implementar en el modelo de seguridad establecido mediante el WAF. El objetivo es hacerlo más eficiente, efectivo y preciso en la protección de las aplicaciones web y la detección de amenazas. A medida que pasa el tiempo, las medidas de seguridad deben evolucionar y adaptarse para hacer frente a los crecientes ataques y vulnerabilidades que afectan a las aplicaciones web.

7. CONCLUSIONES

- Al establecer la línea base de ciberseguridad de la infraestructura tecnológica se logró una referencia clara y completa que sirve como punto de partida para futuras mejoras y medidas de seguridad. La identificación de las capacidades tecnológicas existentes permitió a Seguros Alianza S.A. entender su posición actual en términos de protección contra amenazas cibernéticas, al mismo tiempo resalta las fortalezas que pueden ser potenciadas y las debilidades que requieren atención inmediata.

  En última instancia, la definición de la línea base no solo mejoró la resistencia de la infraestructura tecnológica de Seguros Alianza S.A. ante posibles ataques cibernéticos, sino que también establece un marco para el crecimiento y la evolución segura de sus operaciones digitales.

- La creación del plan de remediación de vulnerabilidades identificadas en la organización representó un paso crucial hacia la mejora significativa de la seguridad y la integridad de su infraestructura tecnológica. Al abordar de manera sistemática las debilidades detectadas el plan propuesto fortaleció la postura de la seguridad de la información.

  Finalmente, la ejecución exitosa de este plan no solo permitió proteger la integridad de la infraestructura tecnológica de la organización, sino que también sienta las bases para un entorno digital más seguro y resistente en el futuro.

- La ejecución exitosa de las fases del plan de remediación demostró ser un paso fundamental hacia la fortificación de la seguridad en la organización. Este proceso meticuloso, diseñado para abordar las vulnerabilidades identificadas según su nivel de criticidad, permitió una mejora sustancial en la resistencia de la infraestructura tecnológica.

- La implementación del cortafuegos de aplicaciones web (WAF) en Seguros Alianza S.A. se configura como un esquema o modelo de infraestructura técnica que proporciona a las organizaciones medianas o grandes las herramientas necesarias para hacer frente a una amplia variedad de amenazas de ciberseguridad que se vuelven cada vez más sofisticadas a medida que avanza la tecnología de la información.
- El modelo de infraestructura del WAF implementado se basa en la adopción y aplicación de estándares y regulaciones que se pueden actualizar de forma continua para adaptarse a los nuevos requisitos establecidos por las organizaciones o las aplicaciones web.
- Los resultados obtenidos durante las pruebas reflejaron una mejora significativa en la protección, detección y análisis del tráfico de red. Estas soluciones de seguridad se posicionan como opciones competitivas para empresas que buscan fortalecer su postura de seguridad.
- La implementación de un WAF permitió contar con diferentes controles que llevan a cabo una mitigación efectiva de los riesgos presentes en la infraestructura de una organización. Es importante destacar la utilidad del WAF, ya que puede adaptarse a cualquier entorno web, brindando protección y seguridad en línea con los estándares y requisitos de la organización.

Referencias

[1] F5 GLOSSARY (2022). ¿Qué es un WAF (Web Application Firewall)? Obtenido de https://www.f5.com/es_es/services/resources/glossary/web-application-firewall

[2] ¿Qué es la Ciberseguridad?: Importancia, tipos de ciberataques y cómo fortalecerla https://www.deltaprotect.com/blog/que-es-la-ciberseguridad#Subtitle-2

[3] F5 GLOSSARY (2022). ¿Qué es la seguridad de las aplicaciones web? Obtenido de https://www.f5.com/es_es/services/resources/glossary/web-application-security

[4] Oracle (2022). ¿Qué es un WAF? Obtenido de https://www.oracle.com/es/database/security/que-es-un-waf.html

[5] Vegagestion (2018). La infraestructura tecnológica: definición, tipos e importancia. Obtenido de https://vegagestion.es/la-infraestructura-tecnologica-definicion-tipos-e-importancia/

[6] Cloudflare (2022). ¿Qué es la seguridad de aplicaciones web? Obtenido de https://www.cloudflare.com/es-es/learning/security/what-is-web-application-security/

[7] Marques (2021). Qué es un WAF y cómo te protege de ciberataques a tus aplicaciones web. Obtenido de https://www.marquesme.com/que-es-un-waf-y-como-te-protege-de-ciberataques-a-tus-aplicaciones-web/

[8] Fortinet (2022). Firewall de aplicación web (WAF) FortiWeb. Obtenido de https://www.fortinet.com/lat/products/web-application-firewall/fortiweb

[9] OWASP: Top 10 de vulnerabilidades en aplicaciones web. Obtenido de https://www.tarlogic.com/es/blog/owasp-top-10-vulnerabilidades-web/

[10] Soluciones WAF en comparación: el Cuadrante Mágico WAF 2018 de Gartner. Obtenido de https://www.consulthink.it/es/soluciones-waf-en-comparacion-el-cuadrante-magico-waf-2018-de-gartner/