Propuesta de implementación de un WAF para la protección de aplicaciones WEB en la empresa Medinistros S.A.S.

Garcia Murillo Miguel Angel, Molina Guzmán Diego Fernando, Rivera Buitrago Oscar Daniel y Romero Rodríguez Endi Jeinner

Especialización En Seguridad Informática, Fundación Universitaria Compensar

Propuesta de Consultoría

Miguel Ricardo Pérez Pereira

27 de noviembre de 2023

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

Propuesta de implementación de un WAF para la protección de aplicaciones WEB en la empresa Medinistros S.A.S.

Garcia Murillo Miguel Angel, Molina Guzmán Diego Fernando, Rivera Buitrago Oscar Daniel y Romero Rodríguez Endi Jeinner

Trabajo de grado presentado como requisito parcial para optar al título de:

Especialistas en Seguridad Informática

Director (a): Jairo Cesar Gomez Acero

Coordinador Académico Programa | Bogotá

Línea de Investigación:

Descriptiva - Consultoría Seminario Grado

Grupo de Investigación:

Especialización en Seguridad Informática

Fundación Universitaria Unipanamericana – Compensar

Facultad de Ingeniería, Ingeniería de (Especialización en Seguridad Informática)

Bogotá D.C., Colombia

2023

Resumen

La creciente amenaza de ciberataques en el ámbito mundial, intensificada por la pandemia de COVID-19, ha impactado significativamente a empresas y organizaciones de diversos sectores. El área de la salud, en particular, ha experimentado un aumento sustancial en la incidencia de ataques cibernéticos. Este fenómeno ha llevado a la urgente necesidad de fortalecer las medidas de seguridad informática en aplicaciones web expuestas a Internet.

Este trabajo de grado, realizado por los autores García Murillo Miguel Ángel, Molina Guzmán Diego Fernando, Rivera Buitrago Oscar Daniel y Romero Rodríguez Endi Jeinner, se presenta como una propuesta de implementación de un Web Application Firewall (WAF) en la empresa Medinistros S.A.S. y su objetivo principal es salvaguardar las aplicaciones web utilizadas en las operaciones diarias de la empresa y mitigar los riesgos de seguridad.

El contexto actual revela que las aplicaciones web son vulnerables a una variedad de amenazas cibernéticas, lo que puede resultar en la pérdida de información valiosa, daño a la reputación de la empresa y consecuencias legales. Los ciberdelincuentes han intensificado sus esfuerzos para explotar estas vulnerabilidades, destacando la necesidad de contar con una defensa efectiva.

El trabajo aborda una serie de pasos clave, que incluyen la identificación de aplicaciones web de acceso público, la investigación y comparación de diferentes tipos de WAF disponibles en el mercado, y la recomendación del WAF más adecuado para Medinistros S.A.S. Además, se exploran los alcances y limitaciones de la propuesta, se presenta un marco teórico que establece los fundamentos de la seguridad informática y los tipos de ataques a aplicaciones web, se describe la implementación de un WAF y se discuten los resultados obtenidos.

Palabras Clave: (Firewall, Vulnerabilidad, Aplicación web)

Abstract

The growing threat of cyber-attacks worldwide, intensified by the COVID-19 pandemic, has significantly impacted companies and organizations in a variety of sectors. The healthcare area has experienced a substantial increase in the incidence of cyber-attacks. This phenomenon has led to the urgent need to strengthen computer security measures in web applications exposed to the Internet.

This degree work, carried out by the authors García Murillo Miguel Ángel, Molina Guzmán Diego Fernando, Rivera Buitrago Oscar Daniel and Romero Rodríguez Endi Jeinner, is presented as a proposal for the implementation of a Web Application Firewall (WAF) in the company Medinistros S.A.S. and its main objective is to safeguard the web applications used in the daily operations of the company and mitigate security risks.

The current context reveals that web applications are vulnerable to a variety of cyber threats, which can result in the loss of valuable information, damage to company reputation and legal consequences. Cybercriminals have intensified their efforts to exploit these vulnerabilities, highlighting the need for effective defense.

The paper addresses a series of key steps, including the identification of publicly accessible web applications, the investigation and comparison of different types of WAFs available in the market, and the recommendation of the most appropriate WAF for Medinistros S.A.S. In addition, the scope and limitations of the proposal are explored, a theoretical framework establishing the fundamentals of computer security and the types of attacks on web applications is presented, the implementation of a WAF is described, and the results obtained are discussed.

Keywords: (Firewall, Vulnerability, Web application)

Contenido

PÁG.

RESUMEN ..... **V**

INTRODUCCIÓN **1**

ANTECEDENTES Y JUSTIFICACIÓN 1
FORMULACIÓN DEL PROBLEMA 2
OBJETIVO GENERAL 3
Objetivos Específicos *3*
ALCANCES Y LIMITACIONES 3

1. MARCO TEÓRICO **4**

1.1 CONCEPTOS BÁSICOS 4
1.1.1 Aplicación Web: *4*
1.1.2 Vulnerabilidad informática: *5*
1.1.3 Firewall: *6*
1.2 WAF (WEB APPLICATION FIREWALL) 6

2. DISEÑO METODOLÓGICO **8**

2.1 IDENTIFICACIÓN DE LAS APLICACIONES WEB: 8
2.2 COMPARACIÓN DE WAF EN EL MERCADO: 8
2.3 RECOMENDACIÓN DEL WAF MÁS ADECUADO: 11

3. RESULTADOS **12**

4. CONCLUSIONES Y RECOMENDACIONES **13**

4.1 CONCLUSIONES 13
4.2 RECOMENDACIONES 13

BIBLIOGRAFÍA **14**

Introducción

Los avances tecnológicos, desde la invención de las computadoras hasta la Inteligencia Artificial y la Red 5G, han convertido los datos en activos cruciales para las organizaciones. Sin embargo, las amenazas cibernéticas sofisticadas y la falta de medidas de seguridad perimetral pueden exponer la información a ataques. El desconocimiento en seguridad informática también contribuye a la vulnerabilidad, especialmente a través de aplicaciones web, lo que puede resultar en pérdidas económicas y daños a la reputación. En este contexto, se propone implementar medidas en Medinistros S.AS. para monitorear y proteger el acceso a las aplicaciones web, mitigando así riesgos y posibles ataques.

Antecedentes y Justificación

El aumento significativo de ciberataques a nivel mundial, atribuido a la pandemia del COVID-19, ha llevado numerosos sectores a enfrentar brechas en sus sistemas informáticos, los ataques cibernéticos experimentan un incremento del 600% (González, 2023). La detección de vulnerabilidades en la seguridad informática suele tardar seis meses en la mayoría de las compañías (Osborne, 2015).

El sector salud, ha sido blanco de un aumento del 90% en los ciberataques a nivel mundial (Frost & Sullivan, 2021). En Colombia COLCERT reportó más de 36 ataques, incluyendo suplantación de sitios web (Mogollón Vargas, 2023), afectando la imagen de empresas como “Empresas Públicas de Medellín, Caracol Tv, Colsanitas, Salud Total”, entre otras (MinTIC, 2022). Además, el centro nacional de ciberseguridad de la policía nacional informó un total de 54.121 denuncias entre enero y octubre de 2021 (Cámara Colombiana de Informática y Telecomunicaciones, 2022).

Dada la vulnerabilidad del sector salud en cuento a infraestructura tecnológica, se destaca la importancia de proteger todos activos de la información. En este contexto, Medinistros S.A.S., es una empresa del sector salud, busca mitigar los riesgos implementando un Web Application Firewall (WAF). Este WAF, basado en OWASP, ofrece un análisis de seguridad para los portales web, identificando vulnerabilidades de alto riesgo en diferentes metodologías de programación web. La implementación de esta herramienta proporcionará a Medinistros S.A.S. una defensa mejorada contra ciberataques en sus portales web.

Formulación del Problema

En el año 1999 nace la empresa Medinistros S.A.S. como solución a diferentes áreas de la salud, estableciendo como objetivo principal ofrecer servicios de alquiler, venta y postventa de equipos y suministros médicos. A través del tiempo y dado el crecimiento de la compañía, la alta gerencia ha establecido estrategias que permitan sistematizar los diferentes procesos, con el fin de llevar el control de los equipos y suministros médicos que manejan dentro de la empresa. (Medinistros, 2022)

Para llevar a cabo su objetivo, la compañía cuenta con un aplicativo interno que maneja la información de clientes, proveedores y colaboradores, de los cuales se almacenan datos confidenciales, dichos datos deben estar bajo una adecuada protección para evitar su filtración, impacto reputacional de la compañía y/o repercutir en problemas legales.

El aplicativo permite el acceso de manera local y externa por una interfaz web que se encuentra ubicada en lo servidores de Medinistros. Dado lo anterior se identifican posibles vulnerabilidades en los datos consultados por la aplicación WEB.

De lo anterior se desprende la siguiente pregunta de investigación, ¿es posible que por medio de la implementación de un WAF se puedan mitigar las potenciales vulnerabilidades a las cuales están expuestas las aplicaciones Web?

Objetivo General

Proponer la implementación del Web Application Firewall (WAF) más adecuado para la empresa Medinistros S.A.S., con el fin de proteger sus aplicaciones web y así mitigar los riesgos de seguridad.

Objetivos Específicos

- Identificar las aplicaciones web de acceso público que utiliza la empresa Medinistros S.A.S., con el fin de protegerlas a través de un Firewall de aplicación Web (WAF).
- Investigar y comparar las distintas clases de WAF del mercado, con el fin de determinar sus principales características y beneficios.
- Recomendar el WAF más adecuado para implementar en la empresa Medinistros S.A.S.

Alcances y Limitaciones

Esta propuesta pretende recomendar a la empresa Medinistros S.A.S. la mejor opción de WAF a implementar en la entidad, con el fin de evitar filtración de información que conlleve a pérdidas económicas o en su defecto afectación de la reputación tanto de la empresa como la de sus clientes. Para esto se hará entrega del estudio realizado con información de características, ventajas y desventajas de los diferentes tipos de WAF.

Para la realización de la consultoría se requiere por parte de Medinistros S.A.S. toda la información correspondiente al uso y a la funcionalidad de los sistemas Web que poseen; la omisión de algún dato puede generar un estudio basado en supuestos, lo que falsearía el resultado de este. Otro limitante es el factor económico, ya que, aunque existen WAF mucho más completos que el recomendado, estos pueden tener un costo muy alto para la empresa, por lo que serían inviables.

1. Marco teórico

A continuación, se presentan detalladamente los conocimientos necesarios para afianzar las bases de entendimiento de las diversas definiciones que están asociadas al WAF y así abordar de manera más amplia el objeto de estudio de la presente propuesta.

1.1 Conceptos básicos

Los ataques cibernéticos son una amenaza creciente para las organizaciones de todos los sectores, incluido el sector salud. En Colombia, los ciberataques aumentaron 133% en 2022 y el sector salud fue uno de los más impactados. (Editorial La República SAS, 2023). Una de las principales vulnerabilidades de las aplicaciones web es la falta de seguridad (Eri Gutiérrez, 2021). Los atacantes pueden identificar esta debilidad para acceder a los datos confidenciales, realizar ataques de denegación de servicio, dañar las aplicaciones web, entre otros.

1.1.1 Aplicación Web:

Software con el que un usuario puede acceder por medio de un navegador de internet, ya sea en la extranet[1] o intranet[2]. Se caracterizan por presentar dinámicamente diferentes servicios como, realizar compras, compartir archivos, enviar y/o recibir correo electrónico, transacciones bancarias, entre otras muchas.

Según [(Amazon Web Service, 2023b)], los principales beneficios de un aplicativo web son:

- ***Accesibilidad***: Las aplicaciones pueden ser accedidas desde cualquier navegador web y desde distintos dispositivos tecnológicos.
- ***Simplicidad***: Enfocada al usuario, sin descarga e instalación, acceso por medio de dirección URL a través de navegador.
- ***Escalabilidad***: Permite mejorar rendimiento con grandes volúmenes de transacciones.

[1] Red privada que hace uso de los protocolos de internet, con el fin de compartir de forma segura información o una operación determinada. (…) Puede configurarse como una internet colaborativa entre compañías o empresas. (Cardador, 2014)

[2] Sitio web interno diseñado para trabajar dentro de una determinada compañía. (Cardador, 2014)

Los ataques más comunes en las aplicaciones Web, según (Gutiérrez Eri, 2021):

- ***Inyección SQL***: Código malicioso para obtener datos de las bases de datos.
- ***Autenticación y gestión de sesiones***: Se busca explotar deficiencias en la aplicación de autenticación y administración de sesiones, para obtener acceso.
- ***Cross-site scripting (XSS)***: Inyección de código malicioso modificando HTML o JavaScript en una página web, con el fin de identificar vulnerabilidades.
- ***Referencias no Seguras***: Se evidencian vulnerabilidades que puedan tener las referencias a los objetos definidos en el código fuente.
- ***Malas prácticas de codificación***: La codificación sino es realizada con buenas prácticas, puede permitir el acceso indebido a los valores de las variables.
- ***Malware***: Software malicioso, el cual busca ser ejecutado en el PC objetivo y así infectarlo otorgando control remoto y acceso a información privilegiada.
- ***Ataques de denegación de servicio (DoS)***: Se busca bloquear el acceso a la aplicación Web, con una masiva cantidad de peticiones que el servidor no logra responder.

1.1.2 Vulnerabilidad informática:

Fallo que presenta un sistema en determinado momento, el cual, puede ser explotado por una persona o sistema (atacante), generando así un potencial riesgo, lo cual ocasiona perdida de información, infección de la red o el bloqueo en los servicios. (Romero & Figueroa, 2018).

Categorización de vulnerabilidades según: (Quiroz Zambrano & Macías Valencia, 2017)

- **Vulnerabilidades conocidas sobre aplicaciones instaladas**: Existen y conllevan a generar una actualización (parche) en el programa para solucionar la debilidad.
- **Vulnerabilidades conocidas sobre aplicaciones no instaladas**: No se refleja en la instalación de la actualización, sino en análisis de código estático de la aplicación.
- **Vulnerabilidades no conocidas**: No es conocida por los desarrolles, por lo tanto, es más factible que sea atacada.

1.1.3 Firewall:

Un firewall o Cortafuegos en español, es un conjunto de dispositivos y aplicaciones o la combinación de ambos, para controlar el tráfico entrante y saliente de una red, agregando una capa de protección a nivel perimetral (Scarfone & Hoffman, 2009).

Los firewalls de software se instalan en un servidor u ordenador, y los firewalls de hardware son dispositivos físicos que se conectan a la red (Cisco Systems, 2023). Los firewalls funcionan basados en reglas, las cuales determinan que tráfico se permite y cual se bloquea, estas reglas se pueden configurar para bloquear el acceso de peticiones sospechosas (García & Fragoso, 2010). En palabras de AO Kaspersky Lab, 2023, los firewalls son una parte esencial de la seguridad de la red, son una de las primeras líneas de defensa contra los ataques cibernéticos.

Tipos de Firewall y sus respectivas categorías: (Anwar et al., 2021):

- **Cortafuegos tradicionales:** Controlan el tráfico que entra o sale de una red.
- **Cortafuegos de Nube:** Son la nueva generación, que filtran tráfico entre máquinas virtuales y sus dispositivos de red. Son más económicos en diseño y dispositivos.
- **Cortafuegos Virtuales:** Primera generación que no era aplicable en hardware, solo en software, y funcionaba como hipervisor usado para proteger un entorno virtualizado.
- **Cortafuegos de próxima generación (NGFW):** Altamente adaptable, al reconocer diferentes categorías de la actividad web, más que todo en la actualización y creación de aplicaciones más sofisticadas y las amenazas maliciosas que estas conllevan.
- **Cortafuegos de Aplicación Web (WAF):** Capa de aplicación y su enfoque está en la seguridad Web (servidores, aplicaciones, cookies, sesiones).

1.2 WAF (Web Application Firewall)

Un Web Application Firewall (WAF) es un dispositivo esencial para la seguridad de las aplicaciones, diseñado para analizar y monitorear componentes clave, con reglas predefinidas y personalizadas para controlar ataques comunes como inyección SQL, XML y scripts. Utilizado

en el Frontend[3], examina las solicitudes antes de llegar al Backend[4], filtrando y analizando conforme a reglas predeterminadas o personalizadas para minimizar vulnerabilidades del código fuente (ESET, 2021; Kurniawan et al., 2018).

Ahora bien, Un WAF tiene varios aspectos importantes a nivel de reglas y directivas que permite establecer una seguridad para las aplicaciones, dichas reglas son:

- **Reglas Predefinidas:** Son un conjunto de reglas o directivas determinadas por OWASP, y cuentan con varias versiones (3.2, 3.1, 3.0 o 2.2.9.), (Microsoft, 2023d) (Amazon Web Service, 2023a), las cuales permiten tener una protección frente al conjunto de amenazas comunes de seguridad en las aplicaciones web, estas se actualizan automáticamente frente a nuevos ataques.
- **Reglas Personalizadas:** Definidas por el usuario, y permiten controlar y evaluar las peticiones que ingresan al WAF de acuerdo con la necesidad de la aplicación, tienen tres condiciones (permitir, denegar o registrar solicitudes) (Microsoft, 2023c) (Amazon Web Service, 2023a)
- **Reglas de detección:** Las reglas de detección identifican patrones de tráfico que son indicativos de ataques. ((Amazon Web Service, 2023a; Microsoft, 2023c, 2023d)
- **Filtrado de contenido:** El filtrado de contenido bloquea el tráfico que contiene contenido dañino, como Malware o código malicioso. (Microsoft, 2023b, 2023c, 2023d)
- **Monitoreo de tráfico:** Permite identificar ataques que no se detectan mediante reglas o filtrado de contenido.

[3] Interfaz gráfica del usuario que permite navegación a través de menús, visualización de imágenes gráficas. En pocas palabras, es donde se permite observar varios elementos o componentes, por ejemplo una página Web (Amazon Web Service, 2023b).

[4] Se encarga de acceder a los datos en servidores, los cuales procesan las solicitudes y/o peticiones realizadas por el usuario a través de una aplicación (Amazon Web Service, 2023b)

2. Diseño Metodológico

En esta sección, se detalla el diseño metodológico que se seguirá para llevar a cabo la propuesta de implementación del WAF en Medinistros S.A.S. Como primera instancia se realizará un estudio que identifique las aplicaciones web de acceso público que utiliza la empresa Medinistros S.A.S., y los posibles riesgos a los que se encuentran expuestas.

2.1 Identificación de las aplicaciones Web:

Después de la investigación realizada en la compañía Medinistros S.A.S se identificaron las siguientes aplicaciones web expuestas a internet:

- www.medinistros.com: Portal principal donde se visualiza la información relacionada de la compañía al público en general, proteger el sitio es importante porque se vería afectada la disponibilidad y la reputación de la compañía al sufrir un ataque.
- www.programa.medinistros.com: Se encuentra publicada la aplicación SAP de la compañía donde se encuentra la información relevante de clientes, EPS y IPS, por lo que es imprescindible la protección con el fin de evitar fugas de información para evitar afectaciones de reputación como legales.
- www.sanroqueips.com.medinistros.com: portal informativo como de contacto de ámbito general de los clientes con dificulta auditiva, por lo que también es necesario proteger el portal para evitar afectación de disponibilidad como reputacional.

2.2 Comparación de WAF en el mercado:

En el mercado se encuentran tres tipos de WAF (Check Point, 2023; RadWare, 2023), su función es mejorar la seguridad de las aplicaciones con el análisis constante del tráfico, estos tipos son:

- **Software:** Es básicamente un dispositivo virtual que puede ser implementado en todas las infraestructuras conocidas (privada, pública o hibrida), aunque su implementación es fácil se deben contemplar costos de mantenimiento o del proveedor que presta el servicio.
- **Hardware:** Está diseñado para aquellas empresas grandes que desean tener este servicio para evitar latencias, su implementación puede ser demasiado costosa por los

componentes adicionales que se deben adquirir, además se debe contratar un especialista para el mantenimiento y administración correspondiente.

- **De Nube:** Es muy popular en la actualidad dado que particularmente tiene lo mejor de los dos modelos hardware (robustes) y software (agilidad), esto quiere decir que cualquier proveedor sea Microsoft, Google, AWS, entre otros permite un despliegue rápido, interfaces amigables y adicionalmente, este modelo cuenta con acceso constante a las actualizaciones que le permite detectar las amenazas más recientes. Es importante tener presente que los costos varían dependiendo del proveedor.

En la tabla 1, se puede visualizar aspectos y características relevantes de cada tipo de WAF, teniendo en consideración la implementación hasta el costo promedio de cada uno en el mercado actualmente, permitiendo tener así un conocimiento global para elegir el mejor para Medinistros S.A.S (AWS, 2023; Google Cloud, 2023; Microsoft, 2023a, RadWare, 2023).

Tabla 1. Comparativo de características de los tres tipos de WAF

Característica	WAF Hardware	WAF Software	WAF Nube
Implementación	» Adecuaciones Físicas, Centro de Datos (Rack, Energía, Comunicación). » Equipo Físico (Appliance). » Configuración completa. » Especialista WAF (Marca).	» Servidores con Hypervisor (Vmare, Hyper-V entre otros). » Especialista WAF (Marca).	» Basada en cada proveedor de nube (AWS, Google Cloud, Azure, Radware, Cloudfire).
Escalabilidad	» Limitada, dado los componentes físicos adquiridos y licencias.	» Aceptable, modificaciones a demanda y licenciamiento.	» Excelente, permite configuración automática o a demanda.
Mantenimiento / Actualizaciones	» Realizada por Especialista.	» Realizada por Especialista.	» Automáticas responsabilidad del proveedor de servicios.
Flexibilidad	» Limitada al componente físico.	» Limitada a configuraciones del software.	» Alta permite tener una flexibilidad de acuerdo a la demanda
Elasticidad	» Limitada componente físico	» Limitada a configuraciones del software.	» Permite tener una elasticidad de acuerdo con la demanda.
Rendimiento	» Ofrece alta velocidad y rendimiento debido a su proximidad física al servidor.	» El rendimiento puede ser más lento que el WAF en hardware, ya que se ejecuta en una máquina virtual.	» Puede variar dependiendo del proveedor de servicios, pero generalmente ofrece un rendimiento sólido.
Infraestructura	» Local.	» Local.	» Proveedor Nube.
Integración con servicios en nube	» Limitada se deben considerar costos adicionales.	» Aceptable, pero se debe considerar costos adicionales.	» Nativa en servicio de nube.
Adaptable	» Grandes organizaciones con alto tráfico de visitantes diarios, que requieren velocidad y rendimiento.	» Organizaciones de tamaño mediano a grande que desean una solución más rentable que el WAF en hardware.	» Organizaciones de todos los tamaños que prefieren externalizar la gestión de seguridad y no desean invertir en hardware.
Costo Promedio Mes	Alto (>$30,000 USD).	Medio (~$15,000 USD).	Bajo (~$1,000 USD al mes).

2.3 Recomendación del WAF más adecuado:

Para hacer frente a los problemas de seguridad cibernética y proteger los activos de información de Medinistros S.A.S., es fundamental contar con un WAF. Esta herramienta actúa como un escudo de ciberdefensa frente a las crecientes ciberamenazas que enfrentan las aplicaciones web de la organización.

Mediante la información obtenida acerca de la infraestructura física-tecnológica, del personal de TI, así como el reconocimiento de las aplicaciones web expuestas a internet que se describen en el diseño metodológico, se propone como solución la adquisición de un WAF de nube.

Esta recomendación se realiza a su vez por las características que tiene el WAF propuesto, permitiendo una implementación y configuración intuitiva, adicionalmente no requiere de personal especializado o que conozca del tema; los mantenimientos y las actualizaciones que se requieran serán realizadas por el proveedor de nube (Azure, Amazon, Google Cloud, Entre otras).

Por otro lado, el WAF de nube tiene unos costos accesibles en comparación a los otros tipos (Software y Hardware). En el siguiente apartado se encontrará un comparativo con los tres proveedores de servicio en nube y un proveedor con un alto prestigio que ofrecen el producto de WAF.

Tabla 2. Comparativa Costos WAF Nube

Características WAF Nube	Costo Mensual Azure	Costos Mensual Google	Costo Mensual Amazon	Costos Mensual Radware
* Reglas OWASP (Top 10) * Reglas Personalizadas * Reglas Bot * Análisis Trafico HTTP / HTTPS	USD 286.48	USD 660.68	USD 1,356.00	USD 638

***Los valores presentados son en dólares.**

La tabla 2 permite mostrar los costos mensuales asociados a cada proveedor con las principales características de un WAF en nube. (AWS, 2023; Google Cloud, 2023; Microsoft, 2023a)

3. Resultados

A partir de la revisión de las aplicaciones web expuestas al usuario final que tiene Medinistros, se pudo evidenciar que los tres aplicativos son importantes para la operación de la empresa. No protegerlos puede conllevar a fuga y/o secuestro de información y a su vez afectar la reputación de la organización y recaer en inconvenientes legales.

Con respecto a la comparación de los tipos de WAF, se puede inferir que la mejor opción depende inicialmente de la infraestructura con la cual cuenta la empresa y el recurso humano que tiene asignado para tal fin. Esto es un punto de partida para la elección de WAF, dado que cada uno es fuerte dependiendo de la necesidad y de las características descritas en el desarrollo metodológico.

Lo anterior permite recomendar a la empresa Medinistros S.A.S. la viabilidad de implementar un WAF en nube dadas las características que se adaptan tanto a la infraestructura como al personal de tecnología. De acuerdo con el comparativo de la **"Tabla 2. Comparativa Costos WAF Nube"** con los diversos proveedores de WAF en nube, se recomienda la adquisición con el proveedor Microsoft Azure dados los bajos costos durante la implementación y la experiencia de usuario en la administración de la herramienta.

4. Conclusiones y recomendaciones

4.1 Conclusión

A través del análisis realizado a Medinistros S.A.S., se puede concluir que la entidad tiene tres aplicaciones web que se encuentran expuestas a internet, en las cuales dos informan acerca de la empresa y una permite la gestión de clientes, lo que conlleva a que la información pueda ser vulnerada por ataques cibernéticos, en vista de lo anterior y basado en la investigación de los tipos de Web Application Firewall (WAF), se considera proponer la implementación de un WAF de Nube, el cual permitirá la protección de las vulnerabilidades más comunes en los aplicativos web, adicional su administración es intuitiva y a un costo accesible.

4.2 Recomendaciones

Se presentan las siguientes recomendaciones para Medinistros S.A.S.:

- Mantener una inversión constante en seguridad cibernética y estar al tanto de las últimas tendencias y amenazas.

- Realizar auditorías de seguridad regulares para identificar nuevas vulnerabilidades y ajustar la configuración del WAF en consecuencia.

- Fomentar la conciencia de seguridad cibernética entre el personal para prevenir ataques basados en ingeniería social.

- Explorar opciones de capacitación y formación en seguridad informática para el equipo técnico.

Bibliografía

Amazon Web Service. (2023a). *AWS WAF rules - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced*. https://docs.aws.amazon.com/waf/latest/developerguide/waf-rules.html

Amazon Web Service. (2023b). *¿Qué es una aplicación web? - Explicación de las aplicaciones web - AWS*. https://aws.amazon.com/es/what-is/web-application/

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences 2021, Vol. 11, Page 9183*, *11*(19), 6–11. https://doi.org/10.3390/APP11199183

AO Kaspersky Lab. (2023). *¿Qué es un firewall? Funcionamiento de los firewalls y tipos de firewalls*. https://latam.kaspersky.com/resource-center/definitions/firewall

AWS. (2023). *Calculadora Precios AWS*. https://calculator.aws/#/addService/WAF

Camara Colombiana de Informatica y Telecomunicaciones. (2022, December 7). *Más de 54.000 denuncias de ciberdelitos se registraron a cierre del tercer trimestre de 2022 - CCIT - Cámara Colombiana de Informática y Telecomunicaciones*. https://www.ccit.org.co/noticias/crecieron-28-las-denuncias-de-ciberataques-a-redes-de-telecomunicaciones/

Cardador, L. (2014). *Implantación de aplicaciones web en entornos internet, intranet y extranet: Vol. Uno* (IC Editorial, Ed.; Primera). IC Editorial. https://books.google.com.mx/books?hl=es&lr=&id=NVYpEAAAQBAJ&oi=fnd&pg=PT3&dq=intranet+extranet&ots=dgj_TJ8ATi&sig=DYmvcfGsunaGEA01axuVuIPwDqQ#v=onepage&q=intranet%20extranet&f=false

Check Point. (2023). *¿Qué es un WAF? - Check Point Software ES Español*. https://www.checkpoint.com/tw/es/cyber-hub/what-is-web-application-firewall/

Cisco Systems. (2023). *¿Qué es un firewall? - Cisco*. https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Editorial La República SAS. (2023). *Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles*. https://www.larepublica.co/empresas/ataques-ciberneticos-en-colombia-han-crecido-30-epm-y-sanitas-son-dos-de-miles-3508452

Eri Gutierrez. (2021). *Identifica Las Principales Vulnerabilidades En Aplicaciones*. https://codster.io/blog/principales-vulnerabilidades-en-aplicaciones/

ESET, W. (2021). *Análisis estático de código fuente orientado a seguridad*. https://www.welivesecurity.com/la-es/2021/01/18/analisis-estatico-codigo-fuente-orientado-a-seguridad/

Frost & Sullivan. (2021, October 21). *US Healthcare Cybersecurity Growth Opportunities*. https://store.frost.com/us-healthcare-cybersecurity-growth-opportunities.html

González, A. (2023). *Ciberdelincuencia creció 600% tras pandemia: Microsoft*. https://dplnews.com/ciberdelincuencia-crecio-600-tras-pandemia-microsoft/

Google Cloud. (2023). *Calculadora de precios de Google Cloud*. https://cloud.google.com/products/calculator#id=f04d879c-aba3-45e6-aa9e-0c6f76418898

Kurniawan, A., Abbas, B. S., Trisetyarso, A., & Isa, S. M. (2018). Static Taint Analysis Traversal with Object Oriented Component for Web File Injection Vulnerability Pattern Detection. *Procedia Computer Science*, *135*, 596–605. https://doi.org/10.1016/j.procs.2018.08.227

Medinistros. (2022). *Medinistros es una compañía que distribuye y comercializa equipos médicos*. https://www.medinistros.com/

Microsoft. (2023a). *Calculadora Precios Azure | Microsoft Azure*. https://azure.microsoft.com/es-mx/pricing/

Microsoft. (2023b, March 10). *¿Qué es el firewall de aplicaciones web de Azure en Azure Application Gateway? - Azure Web Application Firewall | Microsoft Learn*. https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview

Microsoft. (2023c, March 24). *Reglas personalizadas de Firewall de aplicaciones Web de Azure (WAF) v2 en Application Gateway | Microsoft Learn*. https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/custom-waf-rules-overview

Microsoft. (2023d, June 22). *Reglas y grupos de reglas de CRS - Azure Web Application Firewall | Microsoft Learn*. https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=drs21

MinTIC. (2022, December 16). *En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia*. MinTIC. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

Mogollón Vargas, A. (2023, January 10). *FUCS - Fundación Universitaria de Ciencias de la Salud*. https://www.fucsalud.edu.co/noticias/Facultad-de-Ciencias-Administrativas-en-Salud/ataques-ciberneticos

Osborne, C. (2015, May 19). *Most companies take over six months to detect data breaches | ZDNET*. ZD NET. https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias, ISSN-e 2477-8818, Vol. 3, Nº. Extra 3, 2017, Págs. 676-688*, *3*, 13. https://doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

RadWare. (2023). *3 tipos de firewalls de aplicaciones web | Radware*. https://es.radware.com/cyberpedia/application-security/3-types-of-waf/

Romero, M. I., & Figueroa, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES: Vol. Uno* (Área de Innovación y Desarrollo, Ed.; Primera). Área de Innovación y Desarrollo. https://doi.org/http://dx.doi.org/10.17993/IngyTec.2018.46

Scarfone, K., & Hoffman, P. (2009). *Recommendations of the National Institute of Standards and Technology*. 11. https://doi.org/10.6028/NIST.SP.800-41r1

Amazon Web Service. (2023a). *AWS WAF rules - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced*. https://docs.aws.amazon.com/waf/latest/developerguide/waf-rules.html

Amazon Web Service. (2023b). *¿Qué es una aplicación web? - Explicación de las aplicaciones web - AWS*. https://aws.amazon.com/es/what-is/web-application/

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. *Applied Sciences 2021, Vol. 11, Page 9183*, *11*(19), 6–11. https://doi.org/10.3390/APP11199183

AO Kaspersky Lab. (2023). *¿Qué es un firewall? Funcionamiento de los firewalls y tipos de firewalls*. https://latam.kaspersky.com/resource-center/definitions/firewall

AWS. (2023). *Calculadora Precios AWS*. https://calculator.aws/#/addService/WAF

Camara Colombiana de Informatica y Telecomunicaciones. (2022, December 7). *Más de 54.000 denuncias de ciberdelitos se registraron a cierre del tercer trimestre de 2022 - CCIT - Cámara Colombiana de Informática y Telecomunicaciones*. https://www.ccit.org.co/noticias/crecieron-28-las-denuncias-de-ciberataques-a-redes-de-telecomunicaciones/

Cardador, L. (2014). *Implantación de aplicaciones web en entornos internet, intranet y extranet: Vol. Uno* (IC Editorial, Ed.; Primera). IC Editorial. https://books.google.com.mx/books?hl=es&lr=&id=NVYpEAAAQBAJ&oi=fnd&pg=PT3&dq=intranet+extranet&ots=dgj_TJ8ATi&sig=DYmvcfGsunaGEA01axuVuIPwDqQ#v=onepage&q=intranet%20extranet&f=false

Check Point. (2023). *¿Qué es un WAF? - Check Point Software ES Español*. https://www.checkpoint.com/tw/es/cyber-hub/what-is-web-application-firewall/

Cisco Systems. (2023). *¿Qué es un firewall? - Cisco*. https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Editorial La República SAS. (2023). *Ataques cibernéticos han crecido 30% y EPM y Sanitas son dos de miles*. https://www.larepublica.co/empresas/ataques-ciberneticos-en-colombia-han-crecido-30-epm-y-sanitas-son-dos-de-miles-3508452

Eri Gutierrez. (2021). *Identifica Las Principales Vulnerabilidades En Aplicaciones*. https://codster.io/blog/principales-vulnerabilidades-en-aplicaciones/

ESET, W. (2021). *Análisis estático de código fuente orientado a seguridad*. https://www.welivesecurity.com/la-es/2021/01/18/analisis-estatico-codigo-fuente-orientado-a-seguridad/

Frost & Sullivan. (2021, October 21). *US Healthcare Cybersecurity Growth Opportunities*. https://store.frost.com/us-healthcare-cybersecurity-growth-opportunities.html

González, A. (2023). *Ciberdelincuencia creció 600% tras pandemia: Microsoft*. https://dplnews.com/ciberdelincuencia-crecio-600-tras-pandemia-microsoft/

Google Cloud. (2023). *Calculadora de precios de Google Cloud*. https://cloud.google.com/products/calculator#id=f04d879c-aba3-45e6-aa9e-0c6f76418898

Kurniawan, A., Abbas, B. S., Trisetyarso, A., & Isa, S. M. (2018). Static Taint Analysis Traversal with Object Oriented Component for Web File Injection Vulnerability Pattern Detection. *Procedia Computer Science*, *135*, 596–605. https://doi.org/10.1016/j.procs.2018.08.227

Medinistros. (2022). *Medinistros es una compañía que distribuye y comercializa equipos médicos*. https://www.medinistros.com/

Microsoft. (2023a). *Calculadora Precios Azure | Microsoft Azure*. https://azure.microsoft.com/es-mx/pricing/

Microsoft. (2023b, March 10). *¿Qué es el firewall de aplicaciones web de Azure en Azure Application Gateway? - Azure Web Application Firewall | Microsoft Learn*. https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/ag-overview

Microsoft. (2023c, March 24). *Reglas personalizadas de Firewall de aplicaciones Web de Azure (WAF) v2 en Application Gateway | Microsoft Learn*. https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/custom-waf-rules-overview

Microsoft. (2023d, June 22). *Reglas y grupos de reglas de CRS - Azure Web Application Firewall | Microsoft Learn*. https://learn.microsoft.com/es-es/azure/web-application-firewall/ag/application-gateway-crs-rulegroups-rules?tabs=drs21

MinTIC. (2022, December 16). *En el último mes y medio MinTIC ha recibido 36 reportes de ataques cibernéticos en Colombia*. MinTIC. https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/273464:En-el-ultimo-mes-y-medio-MinTIC-ha-recibido-36-reportes-de-ataques-ciberneticos-en-Colombia

Mogollón Vargas, A. (2023, January 10). *FUCS - Fundación Universitaria de Ciencias de la Salud*. https://www.fucsalud.edu.co/noticias/Facultad-de-Ciencias-Administrativas-en-Salud/ataques-ciberneticos

Osborne, C. (2015, May 19). *Most companies take over six months to detect data breaches | ZDNET*. ZD NET. https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/

Quiroz Zambrano, S. M., & Macías Valencia, D. G. (2017). Seguridad en informática: consideraciones. *Dominio de Las Ciencias, ISSN-e 2477-8818, Vol. 3, Nº. Extra 3, 2017, Págs. 676-688*, *3*, 13. https://doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

RadWare. (2023). *3 tipos de firewalls de aplicaciones web | Radware*. https://es.radware.com/cyberpedia/application-security/3-types-of-waf/

Romero, M. I., & Figueroa, G. L. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES: Vol. Uno* (Área de Innovación y Desarrollo, Ed.; Primera). Área de Innovación y Desarrollo. https://doi.org/http://dx.doi.org/10.17993/IngyTec.2018.46

Scarfone, K., & Hoffman, P. (2009). *Recommendations of the National Institute of Standards and Technology*. 11. https://doi.org/10.6028/NIST.SP.800-41r1