ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO DE ARQUITECTURA BASADA EN LA ESTRATEGIA DE SEGURIDAD EN CAPAS PARA UNA EMPRESA PYME DE COMERCIO ELECTRÓNICO EN LA CIUDAD DE GUAYAQUIL"

TESIS DE GRADO

Previa a la obtención del Título de:

MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. YORVIN OSWALDO MIRABA CERCADO

ING. VÍCTOR XAVIER MARCILLO ESPINOZA

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Agradezco en primer lugar a Dios por la oportunidad de alcanzar esta meta en mi vida. A mis padres y hermanos, les estoy agradecido por su apoyo constante y las fuerzas que me brindaron para seguir adelante.

A mi compañero de tesis, por su dedicación y compromiso en el desarrollo y culminación de este proyecto.

Ing. Yorvin Oswaldo Miraba Cercado

AGRADECIMIENTO

Le agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades. A mi esposa e hijos que los amo mucho y fueron el pilar fundamental para continuar y culminar esta maestría. A mis Padres por su confianza, consejos y apoyo incondicional y a mi compañero de Tesis y compañeros de maestría sin el equipo que formamos, no hubiéramos logrado esta meta.

Ing. Víctor Xavier Marcillo Espinoza.

DEDICATORIA

Dedico este trabajo a la memoria de mis abuelos, Rosita Arguello y Fabian Cercado, quienes me inculcaron el amor por el estudio. Aunque ya no estén físicamente, sus espíritus perseverantes y su amor incondicional continúan guiándome en cada paso de mi vida.

Ing. Yorvin Oswaldo Miraba Cercado

DEDICATORIA

Le dedico principalmente a Dios por haberme dado la fortaleza para seguir adelante en momentos de debilidad durante la maestría y darme salud para lograr este nuevo título en mi vida profesional. A mi esposa e hijos que fueron un pilar fundamental brindándome siempre su cariño, comprensión y apoyo emocional. También a mi Padres que con sus consejos me ayudaron a seguir adelante y poder llegar a esta nueva meta profesional.

Ing. Víctor Xavier Marcillo Espinoza.

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO
FREIRE COBO

MGS. LENIN EDUARDO FREIRE COBO

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA
PLUA

MGS.JUAN CARLOS GARCÍA PLÚA

REVISOR

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral”.

Firmado electrónicamente por:
YORVIN OSWALDO
MIRABA CERCADO

ING. YORVIN OSWALDO MIRABA CERCADO

Firmado electrónicamente por:
VICTOR XAVIER
MARCILLO ESPINOZA

ING. VÍCTOR XAVIER MARCILLO ESPINOZA

RESUMEN

El presente trabajo de titulación se llevó a cabo en una empresa de comercio electrónico ubicada en Guayaquil, cuya actividad principal es la venta de productos y servicios a través de Internet. La seguridad de la información es fundamental para proteger tanto los datos de los clientes como los activos de la empresa Por ello, el objetivo central de este estudio fue desarrollar un diseño de arquitectura de seguridad en capas, basado en un análisis de riesgos de los activos de información de la empresa y una evaluación exhaustiva de la seguridad de su infraestructura tecnológica actual.

Para poder llevarlo a cabo, se realizó un análisis de riesgos que incluyó la identificación y evaluación de los activos de información más críticos para la empresa. Este análisis permitió determinar las vulnerabilidades existentes y las posibles amenazas a las que está expuesta la infraestructura tecnológica de la compañía. A partir de estos hallazgos, se desarrolló un diseño de arquitectura de seguridad que incorpora múltiples capas de protección.

La propuesta de este diseño de arquitectura de seguridad en capas no solo protegerá los activos de información de la empresa, sino que también mejorará la confianza de los clientes en la plataforma de comercio electrónico, al saber que sus datos están siendo manejados con los más altos estándares de seguridad. En un entorno digital donde las amenazas cibernéticas están en constante evolución, contar con una estrategia de seguridad robusta y bien estructurada es esencial para el éxito y la sostenibilidad de cualquier empresa de comercio electrónico.

Como resultado, se formularon recomendaciones y un diseño de red de los equipos de seguridad. Estas medidas permitirán a la empresa proteger tanto su red interna como externa, así como el servidor web, salvaguardando la integridad y la confidencialidad de la información crítica.

ÍNDICE GENERAL

ABREVIATURAS Y SÍMBOLOS

DoS: Denegación de Servicio

EDR: Endpoint Detection and Response

HTTP: Protocolo de transferencia de hipertexto

HTTPS: Protocolo De Transferencia De Hipertexto Seguro

IDS: Intrusion Detection System

IP: Internet Protocol

IPS: Intrusion Prevention System

ISO: International Organization for Standardization

SGSI: Sistema de Gestión de Seguridad de la Información

TCP: Transmission Control Protocol

TIC: Tecnologías de Información y de la Comunicación

VPN: Red privada virtual

WAF: Web Application Firewall

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La evolución del comercio electrónico ha traído consigo una serie de desafíos en términos de seguridad. Los cibercriminales están constantemente buscando nuevas formas de vulnerar sistemas y acceder a información sensible. Por lo tanto, las empresas deben estar siempre un paso adelante, adoptando las últimas tecnologías de seguridad y ajustando sus estrategias según las amenazas emergentes. La inversión en ciberseguridad no solo protege los activos de la empresa sino también su reputación y la confianza de sus clientes.

El desarrollo y avance tecnológico da viabilidad a que las empresas ofrezcan productos y servicios de una manera digital, ágil, en línea, buscando satisfacer la demanda y aquellas múltiples necesidades del consumidor, sin embargo, es necesario hacerlo de manera segura, sobre todo cuando se involucran datos informativos de clientes, así como demás información de pagos, esto con la finalidad de reducir la posibilidad de ser víctimas de incidentes de ciberseguridad [1].

Las soluciones de antivirus y firewall resultan insuficientes para garantizar la protección completa de una red empresarial, o para nuestro caso de estudio, una empresa de comercio electrónico. Es necesario mejorar nuestra postura de seguridad, enfocándose tanto en los dispositivos finales como en aquellos que se conectan a internet, y sin dejar atrás a servicios que exponemos a los clientes y que pueden ser accedidos desde internet.

Además de las soluciones tecnológicas, es importante considerar la educación y concienciación del personal. Los empleados deben estar informados sobre las mejores prácticas de seguridad y los posibles riesgos que pueden enfrentar. La capacitación regular y la actualización de conocimientos sobre ciberseguridad pueden ayudar a prevenir incidentes causados por errores

humanos. La combinación de medidas tecnológicas y la educación del personal crea una defensa más sólida contra las amenazas cibernéticas.

Ante lo mencionado, es esencial implementar medidas de seguridad adicionales, con el objetivo de asegurar en los distintos niveles o capas que un atacante podría intentar vulnerar nuestras soluciones o servicios. Cada nivel o capa de seguridad cumple una función específica y trabaja de forma conjunta con las capas adyacentes para garantizar una comunicación segura y confiable entre los sistemas. La implementación de medidas de seguridad en cada capa puede abarcar el cifrado de datos, la autenticación de usuarios, la verificación de la integridad de los datos y la prevención de ataques de denegación de servicio. Con esto se logra una protección más completa y efectiva de la información [2].

.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La empresa se encuentra ubicada en la ciudad de Guayaquil, cuenta con aproximadamente 26 años de experiencia en el mercado donde la principal actividad es la fabricación, comercialización de productos de higiene y productos de limpieza, sean estos hogares, industrias e instituciones públicas o privadas.

La crisis sanitaria derivada de la pandemia de COVID-19 impulsó significativamente la transformación tecnológica en las empresas, fomentando especialmente el crecimiento del comercio electrónico. Esto motivó a empresas que tradicionalmente comercializaban sus productos en establecimientos físicos a expandir su presencia al ámbito digital. Además, ha propiciado la aparición de nuevas empresas que centran exclusivamente sus servicios en el entorno en línea [3].

Los avances tecnológicos han facilitado la incorporación de plataformas de venta en línea. No obstante, los ciberdelincuentes ven estas plataformas como objetivos potenciales debido a la valiosa información que almacena los sitios web de comercio electrónico. Un ataque informático puede resultar en la pérdida no solo de datos, sino también un perjuicio significativo a la confianza del público y la posibilidad de causar daños irreparables.

1.2. Descripción del Problema

Uno de los grandes problemas que enfrentan las pequeñas y medianas empresas son las vulnerabilidades informáticas, que se van formando en la ejecución de sus actividades diarias, estas vulnerabilidades al no ser combatidas, con el tiempo puede causar daños en el funcionamiento laboral de la empresa [4]. Son múltiples los riesgos asociados a equipos y sistemas de información y comunicaciones, ya que cada vez son más los métodos que afectan a la seguridad de la información y las PYMES no cuentan con controles de seguridad. Las vulnerabilidades en las TIC son globales, razón preocupante para grandes, medianas y pequeñas organizaciones, están el espionaje industrial, las violaciones de seguridad, la interrupción de servicios y las fallas en infraestructura y sistemas de información. A lo antes expuesto se suman vulnerabilidades internas y falta de capacitación del personal de cada empresa, los flujos de entrada y salida de personas sin normas de control se convierte un riesgo inherente físico lo que atrasa su desarrollo [5]. En la actualidad la inseguridad informática puede producir en las empresas la pérdida o alteración de la información, que conlleva a ataques cibernéticos para el robo de información, así mismo afectar en el buen funcionamiento de los servicios informáticos y por ende el prestigio de las empresas [4].

De acuerdo con el estudio realizado por Kaspersky Lab, en los últimos 12 meses más de un tercio de los negocios, es decir el 38% han sido afectados por virus y malware causando gran pérdida en la productividad, el 36% se da por el uso inapropiado de recursos por parte de los empleados, de igual manera, uno de cada 5, es decir el 21% han experimentado pérdida de información debido a los ataques de los cuales han sido víctimas; se considera que este tipo de sector se ha convertido en un blanco fácil de ciberataques dada la poca seguridad que dichas organizaciones implementan sobre sus infraestructuras o aplicaciones, se contemplan a continuación algunos de los ataques o eventos más comunes dirigidos a este tipo de organizaciones y su posible mitigación [6].

1.3. Solución Propuesta

El enfoque de seguridad en capas ofrece una defensa más robusta, ya que cada capa agrega una barrera adicional de protección, fortaleciendo la seguridad general de la infraestructura y los servicios en línea. Se considerará el uso de herramientas de seguridad como Firewall, cuyo rol principal es filtrar el contenido de acceso; un WAF diseñado para proteger los sitios web contra posibles ataques; y un sistema anti-DDoS para prevenir ataques de denegación de servicio, además el uso de soluciones de autenticación multi factor que proporciona una capa adicional de seguridad en la verificación de la identidad de un usuario. Esta combinación de medidas contribuye a fortalecer la protección de la infraestructura en línea y garantizar la seguridad de los servicios proporcionados.

El enfoque de seguridad en capas se sustenta con el estudio tomado desde [5], en donde nos presenta una serie de lineamientos que se deben cumplir para brindar seguridad a las pymes:

- Instalar un software antivirus y antimalware confiable.
- Usar cortafuegos de aplicaciones y en capa 4.
- Elegir contraseñas seguras
- Utilizar la autenticación multifactor.
- Actualizar el software de manera regular.
- Cifrar todos los datos confidenciales.
- Asegurar las conexiones Wi-Fi.
- Supervisar los sistemas de pago.
- Mantener el sitio web de la empresa seguro.
- Evitar que los teléfonos móviles sean objetivos de ataque.
- Mantener copias de seguridad de toda la información.
- Hay que recordar que la seguridad física es parte de la ciberseguridad.

1.4. Objetivos

1.4.1. Objetivos General

Elaborar un diseño de arquitectura basado en la estrategia de seguridad en capas que garantice la protección integral de los datos y transacciones en una empresa pyme de comercio electrónico en Guayaquil, mejorando la confianza del cliente y asegurando la continuidad del negocio.

1.4.2. Objetivo Específico

- Analizar el estado actual de la infraestructura y servicios brindados por la empresa dentro del presente estudio.
- Evaluar las vulnerabilidades actuales del sitio web de la empresa para identificar áreas de mejora y fortalecimiento.
- Diseñar la arquitectura objetivo que incluya controles de seguridad para cubrir las vulnerabilidades de la arquitectura actual.

1.5. Metodología

Este proyecto tiene un alcance de tipo descriptivo con un enfoque de estudio no experimental tomando como referencia los dominios de control A9, A10 de la norma ISO/IEC 27002:2013. Estos dominios se enfocan en el control de accesos de los usuarios y el cifrado de información [7].

La entrevista se erige como una herramienta fundamental en el proceso de obtención de información relativa al comercio electrónico, permitiendo el acceso a conocimientos y perspectivas de primera mano por parte de los actores clave en este ámbito. Al mismo tiempo, la investigación documental se convierte en un pilar esencial para la construcción de la arquitectura propuesta, ya que proporciona un sustento sólido a partir de fuentes previamente establecidas, datos históricos y normativas vigentes, permitiendo la formulación de un enfoque estructural y estratégico que refleje tanto la realidad actual como las aspiraciones de crecimiento y desarrollo del comercio en cuestión. Ambas estrategias se complementan de manera sinérgica, garantizando un

enfoque completo y fundamentado en la toma de decisiones relacionadas con el comercio.

Se utiliza la metodología de análisis y gestión de riesgos de los sistemas de información conocida como Magerit conocida como un marco metodológico utilizado en seguridad informática. Desarrollado en España, se centra en identificar, evaluar y gestionar riesgos en sistemas de información. Magerit aborda aspectos técnicos, organizativos y legales para proporcionar una visión integral de la seguridad. Su enfoque sistemático ayuda a las organizaciones a tomar decisiones informadas para proteger sus activos de información.

CAPÍTULO 2

MARCO TEÓRICO

Este capítulo incluye las definiciones de los temas para el desarrollo del presente proyecto de tesis tales como: Pymes de comercio electrónico, seguridad en capas y arquitectura de seguridad.

2.1. Pymes de Comercio Electrónico

Hoy en día el comercio electrónico se ha convertido en una herramienta fundamental para todo tipo de empresas debido a que mueve una gran parte de la economía mundial.

En el Ecuador el 2020 marcó un antes y un después, debido a que la crisis sanitaria obligó a las empresas de comercio electrónico a tener que adaptarse a los cambios tecnológicos para ofrecer sus productos o servicios de una forma más eficiente y directa a sus clientes finales.

El rápido y constante crecimiento de las empresas de comercio electrónico conlleva inevitablemente diversos desafíos, y uno de los más apremiantes es garantizar la seguridad en este ámbito.

Las amenazas cibernéticas dirigidas al comercio electrónico experimentan un aumento constante cada año. Malwares, bots e ingeniería social son solo algunos ejemplos de estas amenazas. Sin una protección adecuada, un comerciante se expone al riesgo de perder información crítica, que abarca desde datos corporativos hasta información de clientes. Esta pérdida potencial puede tener consecuencias devastadoras para la reputación y la estabilidad económica de una empresa. Por ende, la implementación de medidas robustas de seguridad se vuelve esencial para salvaguardar tanto la integridad de los datos como la confianza de los clientes.

Antes de listar las amenazas más comunes, recordemos las siguientes definiciones de vulnerabilidad y amenazas.

2.1.1. Definiciones

Vulnerabilidad. - Se define como una debilidad o falla en el diseño, sistema, aplicación, red, procedimientos o recursos, no anticipada durante el desarrollo de la solución existente, que puede ser aprovechada por actores malintencionados para comprometer la integridad, confidencialidad o disponibilidad de la información.

Amenaza. - En el ámbito digital, una amenaza se refiere a las circunstancias o eventos que pueden tener un impacto negativo en los sistemas informáticos.

Este impacto puede manifestarse de diversas maneras, incluyendo el acceso no autorizado, la destrucción, la divulgación o modificación de la información, así como la denegación de servicios.

Malware. - Es un software malicioso diseñado para infiltrarse en un sistema informático con el propósito de robar datos o fondos, tanto del propietario del sistema como de sus clientes [8].

DoS. - El ataque de denegación de servicio es una táctica utilizada por hackers para saturar un sistema o red con tráfico de manera que se vuelva inaccesible para los usuarios. Este tipo de ataque busca sobrecargar los recursos del sistema, como ancho de banda o capacidad de procesamiento, con el fin de impedir que los servicios normales estén disponibles. La Denegación Distribuida de Servicio constituye en una variante más sofisticada de los ataques DoS. En este caso, la táctica implica el uso de múltiples sistemas para lanzar el ataque, lo que hace que sea más difícil de mitigar. Los sistemas utilizados para la ejecución del ataque, generalmente comprometidos mediante malware, se agrupan en una red botnet controlada por el atacante.

Ingeniería social. - Se trata de una técnica empleada por ciberdelincuentes con el propósito de ganarse la confianza del usuario y persuadirlo a realizar acciones bajo su manipulación y engaño. Estas acciones pueden abarcar desde la ejecución de programas maliciosos hasta la divulgación de claves privadas o la realización de compras en sitios web fraudulentos [9].

Fraude financiero. - El fraude financiero se considera a menudo el tipo de ataque más sensible, ya que tiene como objetivo robar activos financieros de los comerciantes. En el escenario más sencillo, un atacante utiliza datos de tarjetas de crédito robadas para hacer una compra no autorizada en una tienda digital [8].

E-skimming.- Cualquier empresa que acepte pagos en línea puede convertirse en víctima de un e-skimming (o skimming en línea), y aparentemente, las empresas de comercio electrónico no son una excepción.

Por ejemplo, los atacantes pueden insertar código malicioso en los sitios de procesamiento de tarjetas de pago o comercio electrónico para capturar información de tarjeta de crédito de un cliente y robar dinero o hacer una compra no autorizada [8].

Bots.- Los bots maliciosos automatizados representan otra amenaza que puede perjudicar a un negocio de comercio electrónico. Los atacantes tienen la capacidad de inyectar bots en sitios de comercio electrónico con el propósito de asumir el control de las cuentas de los clientes, robar información de tarjetas de crédito, o realizar raspado de precios y contenido de un comerciante [8] .

API attacks.- Los ataques a API se refieren a actividades no autorizadas o maliciosas dirigidas a las interfaces de programación de aplicaciones (API). Las API son conjuntos de reglas y protocolos que permiten que diferentes

aplicaciones de software se comuniquen e interactúen entre sí. A medida que las API se vuelven cada vez más integrales para las aplicaciones y sistemas modernos, también se convierten en posibles objetivos para diversas amenazas cibernéticas [8].

2.1.2. Seguridad en capas

La implementación de medidas de seguridad en distintos niveles o capas tiene como objetivo proteger de manera integral la información y los recursos de la red, cada capa cuenta con su propio conjunto de protocolos y funciones, esto implica abordar amenazas y vulnerabilidades específicas en cada una de estas capas.

Modelo TCP/IP

El modelo TCP/IP consiste en un conjunto de normas estandarizadas. Se compone de cuatro capas: enlace de datos, red, transporte y aplicación, que posibilitan la comunicación entre dispositivos en una red, como Internet.

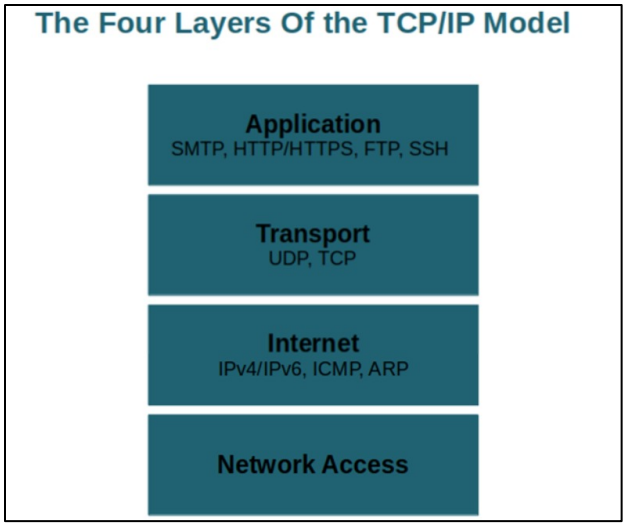


Figura 1. Capas del modelo TCP/IP [10]

A continuación, se resaltan algunos elementos esenciales vinculados a la seguridad en este modelo.

- **Acceso a la red.** – Esta capa se ocupa de las conexiones físicas o inalámbricas de los equipos, incluyendo el control de acceso a la infraestructura tecnológica y al cableado. Como medidas de seguridad se recomienda implementar.
- **Seguridad Física**: Control de acceso a dispositivos de red físicos.
- **Control de Acceso a la Red (nivel de enlace):** autenticación y autorización de dispositivos en la red local.
- **Internet.** - Esta capa se encarga de la transferencia de datos de un nodo de red a otro a través de la red global, como internet. Para la protección en esta capa es recomendable.

- Firewalls para el filtrado de paquetes y VPN para conexiones seguras a través de redes publica o no seguras como la internet.

- **Trasporte. -** Permite la comunicación bidireccional. Protocolos como TCP y UDP operan en esta capa, siendo responsables de facilitar la comunicación a la capa de aplicación. En esta capa se recomienda el uso de protocolos como TLS/SSL que permiten cifrar la comunicación entre dispositivos.

- **Aplicación. -** Es la responsable de facilitar el intercambio de datos a través de aplicaciones como navegadores web o clientes de correo electrónico. Dependiendo del tipo de servicio, se utilizará un protocolo específico para la comunicación. Para la protección de esta capa se debe implementar seguridad que permitan proteger las aplicaciones y servicios que se encuentren publicados en la internet.

2.2. Sistema de Gestión de Seguridad de da Información

2.2.1. ISO 27001

Es una norma elaborada por la Organización Internacional de Normalización (ISO) que detalla la forma de administrar la seguridad de la información en una organización. Su versión más reciente fue lanzada en 2013 y ahora se conoce con el nombre completo de ISO/IEC 27001:2013 [10] .

Esta norma proporciona un marco para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) en el contexto de los riesgos generales del negocio. Está diseñada para

ser adaptable a diversos tipos y tamaños de organizaciones y se centra en garantizar la confidencialidad, integridad y disponibilidad de la información.

2.3. Arquitectura de Seguridad

La arquitectura tiene un papel fundamental en la implementación de la ciberseguridad dado que establece una estructura y un marco para diseñar, implementar y administrar de manera segura los sistemas y redes de una organización.

Contar con una buena arquitectura de seguridad permite mantener la confidencialidad, integridad y disponibilidad de los datos. De igual forma, la arquitectura debe ser lo suficientemente flexible para adaptarse y proporcionar protección ante amenazas cibernéticas en constante evolución.

A continuación, se detallan los equipos y aplicaciones que brindan seguridad.

2.3.1. Firewall

Es un componente de seguridad que puede manifestarse como un dispositivo físico o un software. Su propósito es gestionar el tráfico de red entrante y saliente, siguiendo un conjunto de reglas y políticas predefinidas. Su función principal consiste en autorizar o denegar el tráfico de datos basándose en diversos criterios, como la dirección IP de origen, la dirección IP de destino, el número de puerto y el protocolo utilizado [11].

2.3.2. Waf

Es un dispositivo ubicado en el perímetro de la red, específicamente diseñado para examinar el tráfico entrante y saliente de las aplicaciones web. Su objetivo principal consiste en examinar y filtrar el tráfico web para brindar protección contra amenazas tales como la inyección SQL, ataques de secuencias de comandos en sitios (XSS) y la falsificación de solicitudes entre sitios (CSRF) [12].

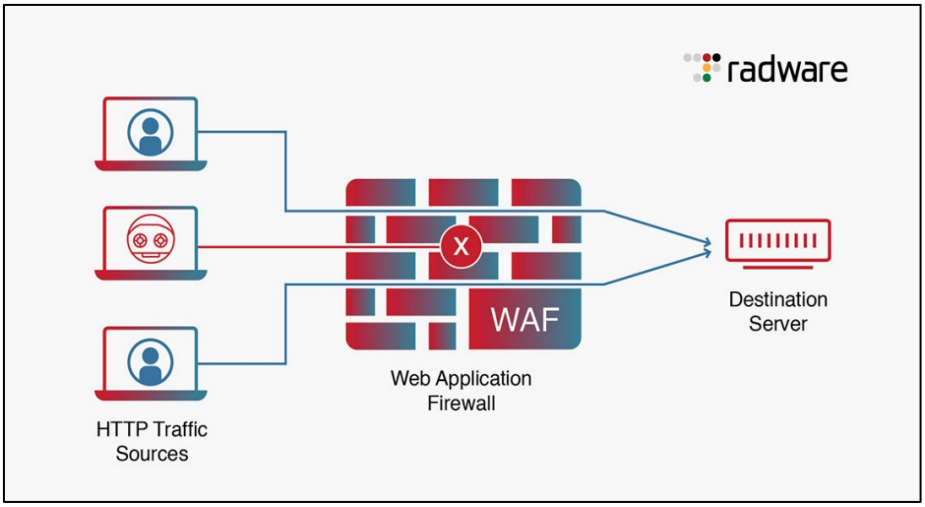


Figura 2 Web Application Firewall (WAF) [14]

2.3.3. Anti DDoS

Un sistema contra ataques DDoS (Distributed Denial of Service) o contra ataques de denegación de servicio distribuido es una solución cuyo propósito es reducir o evitar los impactos de los ataques DDoS. Estos ataques tienen como objetivo saturar los recursos de un sistema, red o servicio, con el fin de hacerlo inaccesible para los usuarios legítimos [13].

2.3.4. Edr

Conocida como detección y respuesta a amenazas de endpoints, constituye un conjunto de herramientas que monitoriza de manera continua los endpoints para identificar y responder a ciber amenazas maliciosas. Las soluciones EDR llevan a cabo una investigación exhaustiva de las amenazas, proporcionando información detallada sobre lo sucedido, el impacto generado y las acciones recomendadas. Al aislar la amenaza en el endpoint, contribuye a eliminarla antes de que pueda propagarse y causar mayores perjuicios[14].

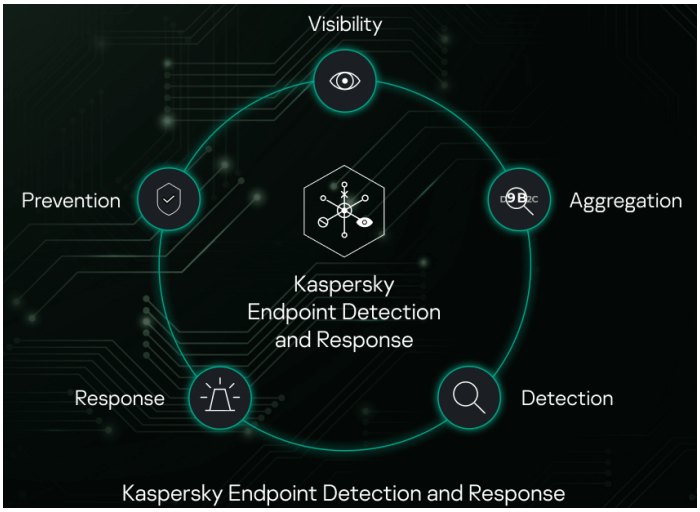


Figura 3 Kaspersky Endpoint Detection and Response (EDR). [17]

2.3.5. Ids

Es una herramienta de monitoreo pasivo para detectar amenazas de ciberseguridad en una organización, que reconoce patrones de comportamiento inusuales. Utiliza algoritmos sofisticados y técnicas de análisis de datos. Al detectar estos comportamientos anómalos, la herramienta emite notificaciones

en tiempo real, alertando a los administradores del sistema sobre posibles amenazas o irregularidades y se tome medidas correctivas.[15].

CAPÍTULO 3

ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1. Contexto de la Organización

La empresa tiene una trayectoria de más de 26 años en el mercado laboral, con sede en la ciudad de Guayaquil, la cual está conformada de diversos departamentos que desempeñan roles clave en el funcionamiento integral. Actualmente, estos departamentos incluyen Gerencia General, Contabilidad, Ventas, Facturación y Bodega, cada uno desempeñando un papel crucial en las operaciones diarias.

Inicialmente se dedicaban a la fabricación y venta de productos químicos para la higiene tanto a hogares, como a industrias e instituciones públicas y privadas. En los últimos 7 años la empresa tomó la iniciativa de diversificar su oferta de portafolio de productos a través de un portal web y la formación de alianzas estratégicas con otras organizaciones, lo que ha resultado en una expansión significativa de su segmento de mercado. Este enfoque estratégico no solo ha consolidado la presencia en el mercado,

sino que también facilitó el proceso de importación de productos bajo su propia marca, llevándola a posicionarse en el mercado nacional.

Es importante señalar que la empresa no cuenta con un departamento específico de infraestructura tecnológica. Incorporar este departamento podría ser beneficioso para gestionar y mantener la infraestructura tecnológica de la empresa, abarcando aspectos como redes, sistemas informáticos, seguridad cibernética y tecnologías emergentes.

3.2. Recopilación de Información

En la identificación de activos de información, se llevó a cabo una visita a las instalaciones de la organización con el fin de realizar una entrevista al Gerente General con el objetivo de identificar los activos con lo que cuenta en su infraestructura tecnológica y elaborar el diseño de red actual ya que no cuenta con un departamento que administra la infraestructura tecnológica de la organización.

En este proceso, hemos identificado que la organización cuenta con un servidor de base de datos donde almacena información sensible y crítica. Se ha observado que realizan semanalmente la copia de respaldo de esta información hacia otro servidor de base de datos secundario en la nube. Para la comunicación utilizan routers y switches que facilitan la conectividad en la red, y cuentan con puntos de acceso wifi para proporcionar conexión inalámbrica en las diferentes áreas de la organización. Adicional cuentan con un servidor de correo, sitio web administrado por un proveedor de Hosting sin ningún tipo de protección de seguridad.

De acuerdo con la información recopilada de los activos se busca establecer estrategias de seguridad efectivas, asegurando la integridad, confidencialidad y disponibilidad de la información, además de fortalecer la protección de su infraestructura tecnológica ante posibles amenazas y riesgos cibernéticos.

Con base a la recopilación de información se levanta el diagrama de la infraestructura actual.

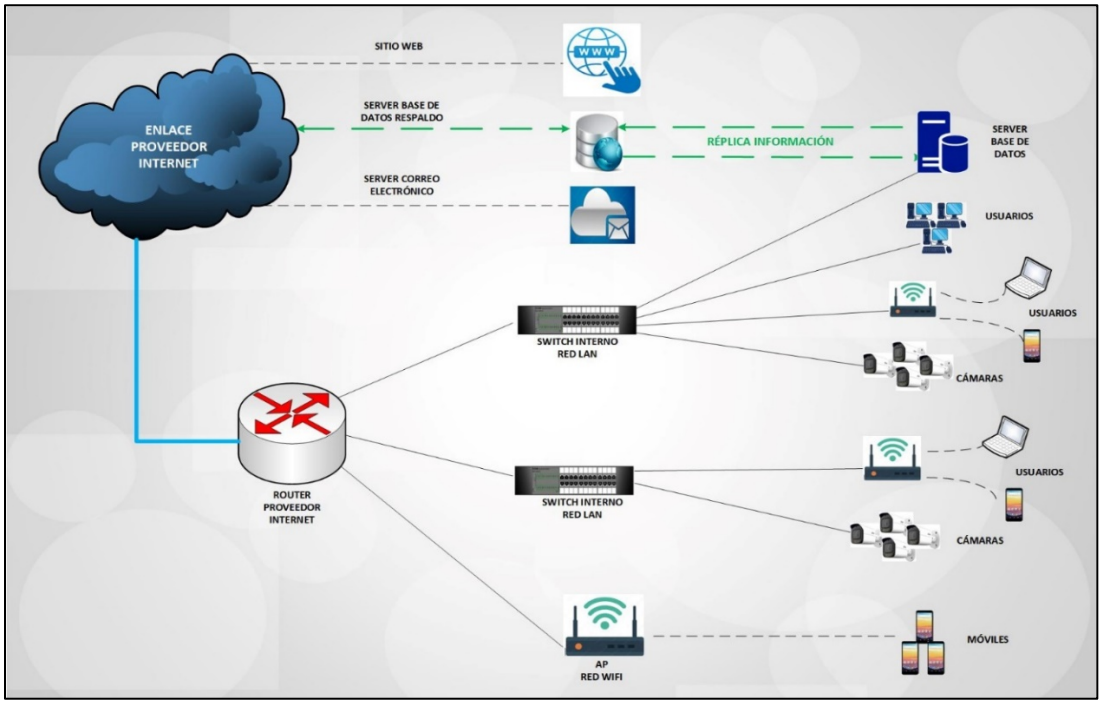


Figura 4 Diagrama actual. Fuente: Autor

3.2.1. Identificación de activos

Para categorizarlos se ha empleado la norma de Magerit versión 3.

A continuación, se muestra el inventario de activos de la organización identificados en el capítulo 3:

Num	Código	Descripción Activos	Tipo
1	SW	Servidor de Base de datos	Información
2	SW	Servidor de Base de datos cloud	Información
3	SW	Servidor Web (Hosting)	Información
4	SW	Servicio de correos	Información
5	HW	Routers	Hardware
6	COM	Switches	Comunicaciones

7	COM	Access Point	Comunicaciones
8	HW	Laptop	Hardware
9	HW	PC de escritorio	Hardware
10	HW	Cámaras IP	Hardware
11	P	Servicios de Soporte externo	Contrato

Tabla 1 Identificación de activos Fuente Autor

3.3. Situación de los Activos de la Información

Luego de recopilar la información sobre los activos de información de la organización, hemos identificado diversas deficiencias que podrían exponer a la empresa a posibles ataques informáticos.

- La carencia de un equipo de seguridad perimetral que lleve a cabo el análisis de tráfico entrante/saliente y el filtrado de contenido representa una brecha significativa en las medidas de seguridad ya que el equipo de seguridad perimetral desempeña un papel esencial al examinar el tráfico entrante y saliente de la red, identificando posibles riesgos y filtrando contenido malicioso.

- La ausencia de segmentación en la red interna, donde no se establece una separación por departamentos, implica que la red interna y la de invitados comparten conectividad y acceso directo entre sí. Esta falta de aislamiento entre distintas áreas de la red podría aumentar significativamente el riesgo de accesos no autorizados y comprometer la seguridad general del entorno. La segmentación de red por departamentos es esencial para limitar el alcance de posibles amenazas y garantizar una protección más efectiva contra accesos indebidos y ataques cibernéticos.

- En relación con los servicios de correo electrónico y el portal web, se ha identificado una carencia significativa al no contar con un equipo de seguridad

dedicado. Esta ausencia podría dejar expuestos los sistemas y datos asociados al portal a amenazas que pueden causar un ciberataque.

- La falta de un acuerdo de confidencialidad con los proveedores externos encargados del soporte de los equipos internos se presenta como una vulnerabilidad significativa en la gestión de la seguridad de la información. La ausencia de estos acuerdos podría exponer a la empresa a riesgos considerables en lo que respecta a la protección de datos y propiedad intelectual.

Estas deficiencias no solo representan riesgos potenciales para la integridad y seguridad de los datos de la empresa, sino que también podrían comprometer la continuidad operativa y la reputación de la organización.

CAPÍTULO 4

EVALUACIÓN DE LA SEGURIDAD ACTUAL

4.1. Soluciones de Seguridad Web

Las soluciones de seguridad web desempeñan un papel fundamental en salvaguardar los sistemas y datos en un entorno digital. Los equipos de seguridad permiten controlar el tráfico mediante reglas, desempeñando una función esencial al controlar el tráfico, estableciendo barreras y filtros que actúan como defensas ante posibles amenazas cibernéticas. Sin embargo, la efectividad de estas medidas no puede darse por sentada. Para garantizar que las soluciones de seguridad se apliquen de manera efectiva y cumplan con su propósito, es imperativo llevar a cabo escaneos regulares. Estos escaneos desempeñan un rol crucial al permitir la detección y la identificación de vulnerabilidades y debilidades que podrían representar puntos de vulnerabilidad en el sistema. El resultado de estos análisis permite una visión detallada de posibles áreas de riesgo, permitiendo a los administradores de seguridad abordar y corregir cualquier brecha de seguridad antes de que pueda ser explotada por amenazas externas.

Herramientas

- **Burp Suite:** Es una herramienta que facilita la realización de pruebas de seguridad en aplicaciones web. Dispone de una versión gratuita, conocida como Burp Free, y una versión de pago denominada Burp Professional.
- **Acunetix:** La herramienta permite la ejecución de análisis automatizados y manuales de vulnerabilidades en aplicaciones web, con el propósito de identificar posibles errores de seguridad que podrían comprometer la integridad de la página web expuesta en internet.
- **Nessus:** Es una de las herramientas más completas del mercado, permitiendo llevar a cabo el escaneo de vulnerabilidades en sistemas informáticos y redes.
- **Nmap:** Es una herramienta de código abierto utilizada para escanear redes y sus puertos. Esta aplicación se emplea comúnmente para realizar auditorías de seguridad y supervisión de redes.
- **Metasploit:** Es utilizado por profesionales de la seguridad de la información, así como por ciberdelincuentes, con el fin de descubrir, explotar y validar vulnerabilidades en sistemas. Se trata de una plataforma respaldada tanto por una comunidad de código abierto como por Rapid7.
- **Qualys SSL Labs :** Es una herramienta en línea sin costo que se ha creado con el propósito de examinar la seguridad de sitios web. Brinda a las organizaciones la posibilidad de analizar la seguridad de sus certificados SSL/TLS y identificar posibles vulnerabilidades.
- **SonarQube:** La plataforma posibilita la revisión del código fuente en busca de errores, vulnerabilidades y prácticas de programación deficientes. Asimismo,

ofrece informes detallados y recomendaciones para mejorar la calidad del código.

- **Mozilla Observatory**: Es una plataforma de código abierto desarrollada por Mozilla que nos permitir de forma gratuita escanear el sitio web e informarnos de la seguridad, buenas prácticas de programación de cualquier sitio web y mostrar los resultados con una ponderación que va desde la A como seguridad máxima hasta la F seguridad deficiente.

4.2. Revisión y Análisis de Resultados

En este apartado brindaremos detalles de las revisiones y análisis de los resultados ejecutados a los activos de información y al sitio web, donde utilizamos varias herramientas mencionadas en el presente capítulo para llevar a cabo estas tareas.

Para testear la seguridad y buenas prácticas de programación del sitio web empresarial empleamos herramientas tales como web Mozilla HTTP Observatory, NMAP para escaneo de puertos y Nessus para escaneo de vulnerabilidades.

En la ilustración 5 y 6 se detallan varias incidencias del resultado al sitio web desde Observatory mozilla.

Observatory Mozilla

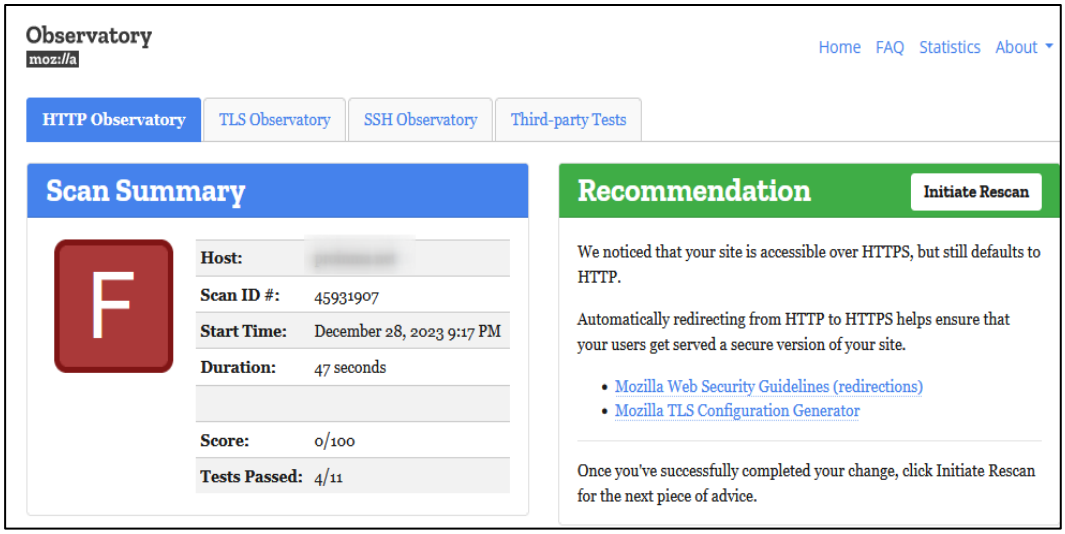
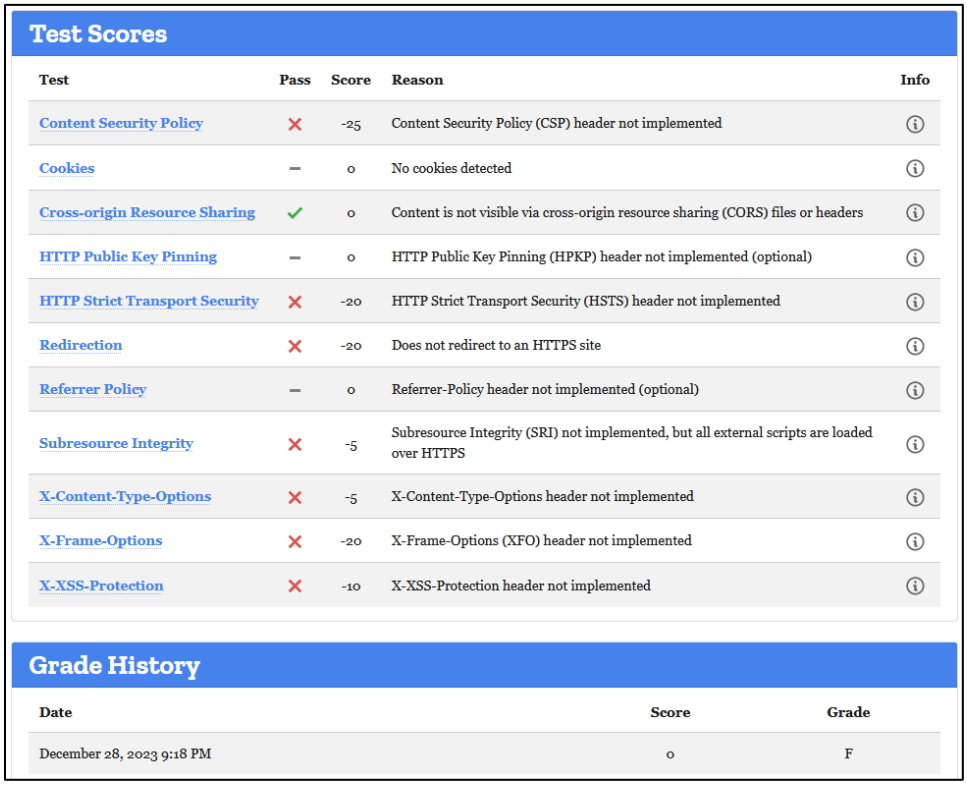


Figura 5:Escáner de página web [16]



Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	
Cookies	–	0	No cookies detected	
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	
Redirection	✗	-20	Does not redirect to an HTTPS site	
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	
Subresource Integrity	✗	-5	Subresource Integrity (SRI) not implemented, but all external scripts are loaded over HTTPS	
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	

Grade History

Date	Score	Grade
December 28, 2023 9:18 PM	0	F

Figura 6 Escáner de página web [19]

Política de seguridad de contenido

No se ha configurado correctamente la política de seguridad de contenido, conocida como Content Security Policy (CSP). La Content Security Policy es una capa adicional de seguridad que ayuda a prevenir ataques como la inyección de scripts maliciosos (XSS) y otros tipos de ataques relacionados con la manipulación del contenido de la página web. Esta política se especifica a través del encabezado HTTP llamado "Content-Security-Policy".

Cuando el encabezado CSP no está implementado o está configurado de manera insuficiente, el sitio web puede ser más vulnerable a ciertos ataques, ya que no se establecen restricciones adecuadas sobre el origen y el tipo de contenido permitido.

Seguridad de transporte estricta HTTP

No se ha implementado el encabezado de seguridad opcional llamado HTTP Public Key Pinning (HPKP).

HTTP Public Key Pinning es un mecanismo de seguridad que permite a un sitio web especificar una lista de claves públicas de certificados que el navegador debe esperar al interactuar con ese sitio en el futuro. Este mecanismo ayuda a proteger contra ataques en los que un atacante intenta usar un certificado SSL/TLS fraudulento para comprometer la comunicación segura.

Es importante tener en cuenta que HPKP ha sido desaconsejado (deprecated) en el estándar HTTP debido a posibles problemas y riesgos asociados con su implementación. La recomendación general es no utilizar HPKP y, en su lugar, confiar en otras medidas de seguridad, como los certificados SSL/TLS correctamente

configurados. Por lo que es ideal conexiones seguras mediante HTTPS y asegurarte de mantener tus certificados actualizados.

Redireccionamiento

Esto significa que al intentar acceder a un sitio web, la conexión no se redirige automáticamente a la versión segura del protocolo de transferencia de hipertexto, conocido como HTTPS.

HTTPS proporciona una capa de seguridad adicional cifrando la comunicación entre el navegador del usuario y el servidor web. Esta encriptación ayuda a proteger la privacidad y la integridad de los datos transmitidos, evitando que terceros intercepten o manipulen la información durante la transferencia.

Cuando un sitio web no redirige automáticamente a HTTPS, los usuarios pueden acceder al sitio utilizando la versión no segura (HTTP) en lugar de la segura (HTTPS). Esto puede dejar la información transmitida vulnerable a posibles ataques, especialmente en entornos donde la seguridad es crucial, como el intercambio de información confidencial, credenciales de usuario, etc

Integridad de los subrecursos

La integridad de subrecursos (SRI) no está implementada, pero todos los scripts externos se cargan a través de HTTPS" indica que, aunque todos los scripts externos en la página web se cargan mediante el protocolo seguro HTTPS, aún no se ha implementado la funcionalidad de Integridad de Subrecursos (SRI).

La Integridad de Subrecursos (SRI) es una medida de seguridad que permite a los desarrolladores garantizar que los recursos externos (como scripts, estilos, fuentes, etc.) que están siendo referenciados desde su sitio web no han sido alterados maliciosamente. Se logra mediante la inclusión de un código hash criptográfico en la etiqueta del recurso, y el navegador verifica que el recurso descargado coincide con ese hash antes de ejecutarlo o aplicarlo.

X-Content-Type-Options

El encabezado X-Content-Type-Options no está implementado", se refiere a la falta de configuración de un encabezado de seguridad específico llamado "X-Content-Type-Options" en el servidor web.

El encabezado X-Content-Type-Options es utilizado para controlar cómo los navegadores web deben interpretar el tipo de contenido (MIME type) de una respuesta recibida desde el servidor. Su objetivo principal es mitigar ciertos tipos de ataques, especialmente aquellos relacionados con la interpretación insegura del tipo de contenido.

X-Frame-Options

Se refiere a la ausencia de configuración del encabezado de seguridad denominado "X-Frame-Options" en el servidor web. El encabezado X-Frame-Options se utiliza para controlar si un navegador web debe permitir o no que la página web sea mostrada dentro de un elemento.

Esta medida de seguridad ayuda a prevenir ataques de secuestros de clic (clickjacking), donde un atacante intenta engañar al usuario para que interactúe con contenido malicioso oculto detrás de un marco invisible o transparente.

Protección X-XSS

Hace referencia al encabezado de seguridad llamado "X-XSS-Protection". Este encabezado es utilizado para ayudar a mitigar ataques de Cross-Site Scripting (XSS) en aplicaciones web.

Los ataques de XSS ocurren cuando un atacante inserta código malicioso (generalmente JavaScript) en una página web, y este código se ejecuta en el navegador de un usuario desprevenido. El encabezado X-XSS-Protection es compatible con algunos navegadores y se puede configurar con varios valores, pero el valor comúnmente utilizado es "1; mode=block". Esto activa el filtro XSS incorporado en el navegador y le indica que bloquee la carga de la página si detecta un intento de ataque XSS.

Escaneo de puertos abiertos con Nmap

En la ilustración 7 se muestra el resultado del escaneo de puertos realizado con la herramienta de código abierto NMAP. En este análisis, se encontraron varios puertos abiertos, incluyendo los puertos 21, 80, 110, 53, y 26 TCP. La presencia de estos puertos abiertos representa un riesgo significativo, ya que pueden ser aprovechados por hackers para intentar obtener acceso no autorizado al servidor. Una vez dentro, los atacantes podrían acceder a información sensible, lo que les permitiría explorar y

comprometer otras áreas privilegiadas de la empresa. Esta vulnerabilidad no solo pone en peligro los datos críticos almacenados en el servidor, sino que también puede servir como punto de entrada para una intrusión más profunda en la red interna, exponiendo a la organización a amenazas mayores como el robo de datos, el sabotaje de sistemas, o la instalación de malware. Por lo tanto, es crucial implementar medidas de seguridad adecuadas, como el cierre de puertos no esenciales, la actualización regular de software y la realización de auditorías de seguridad periódicas, para mitigar estos riesgos y proteger la infraestructura de la empresa.

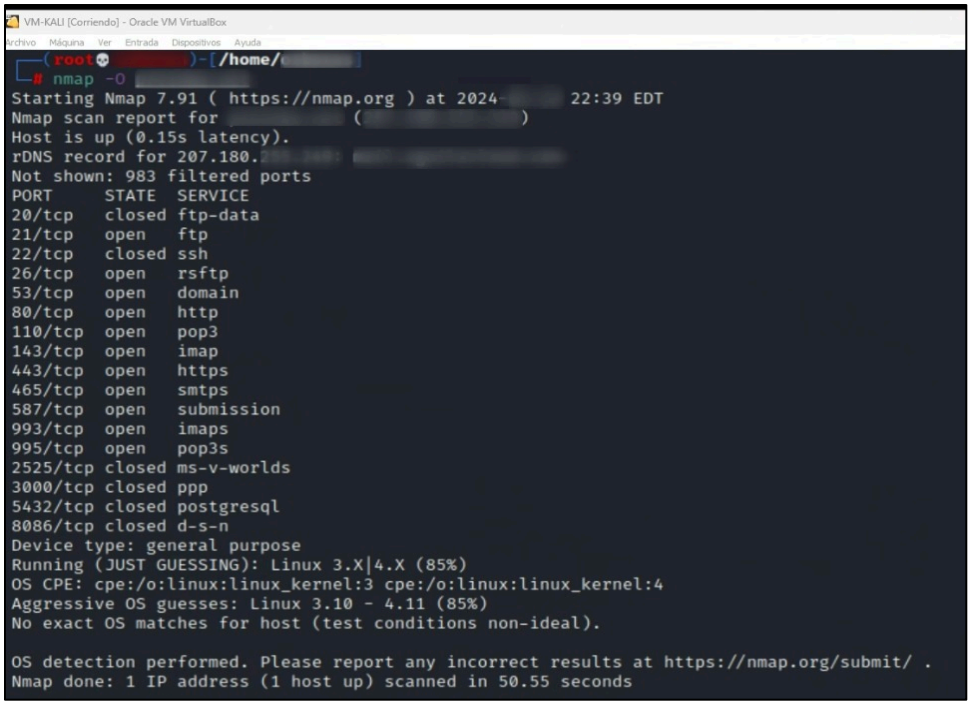


Figura 7 Escáner de puertos abiertos con Nmap Fuente: Autor

Escaneo de vulnerabilidades con Nessus

El análisis de seguridad realizado ha identificado un total de 12 vulnerabilidades en el portal web, todas clasificadas con una severidad de nivel "INFO". Estas vulnerabilidades incluyen la enumeración de plataformas comunes (CPE), detección del tipo y versión de servidores HTTP, escaneo de puertos, y varias detecciones de servidores de correo electrónico como POP y SMTP, entre otros. Aunque ninguna de estas vulnerabilidades representa un riesgo inmediato, su presencia indica áreas donde la seguridad puede ser mejorada para prevenir posibles explotaciones. Por ejemplo, la identificación de versiones específicas de servidores y servicios activos proporciona información que podría ser utilizada por atacantes para encontrar puntos débiles. Además, la detección de cookies web expiradas puede implicar problemas de gestión de sesiones que podrían ser explotados en ataques más sofisticados.

0	0	0	0	12
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 12

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10919	Open Port Re-check
INFO	N/A	-	10185	POP Server Detection
INFO	N/A	-	54580	SMTP Authentication Methods
INFO	N/A	-	10263	SMTP Server Detection
INFO	N/A	-	42088	SMTP Service STARTTLS Command Support
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	14773	Service Detection: 3 ASCII Digit Code Responses
INFO	N/A	-	100669	Web Application Cookies Are Expired

* indicates the v3.0 score was not available; the v2.0 score is shown

Figura 8 Escáner de puertos abiertos con Nessus Fuente: Autor

4.3. Identificación de Riesgos

Posterior a la recopilar información sobre los activos más significativos, se crean tablas en las que se identifican las amenazas y vulnerabilidades de los activos de información según la normativa de MAGERIT versión 3.

4.3.1. Identificación de las Amenazas Y Vulnerabilidades

La amenaza se define como una situación que podría desencadenar un incidente no deseado, con la posibilidad de causar daño a un activo informático o a una organización. Tomando como referencia la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Magerit, se han identificado las amenazas que podrían afectar a los activos de la organización, las cuales se encuentran detalladas en la Tabla 2.

Descripción	Amenazas
Servidor de Base de datos	[A.11]Acceso no autorizado
	[A.15] Modificación deliberada de la información
	[E.19] Fugas de información
Servidor de Base de datos cloud	[A.11]Acceso no autorizado
	[E.19] Fugas de información
	[A.6] Abuso de privilegios de acceso
Servidor Web (Hosting)	[A.11]Acceso no autorizado
	[A.24] Denegación de servicio
	[E.15] Alteración accidental de la información
Servicio de correos	[E.19] Fugas de información
	[A.5] Suplantación de la identidad del usuario
	[A.9] [Re-]encaminamiento de mensajes
Routers	[A.11]Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
	[A.24] Denegación de servicio
Switches	[A.11]Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
	[I.8] Fallo de servicios de comunicaciones
Access Point	[A.11]Acceso no autorizado
	[E.4] Errores de configuración
	[A.6] Abuso de privilegios de acceso
Laptop	[A.11]Acceso no autorizado
	[A.6] Abuso de privilegios de acceso
	[E.25] Pérdida de equipos
PC de escritorio	[A.26] Ataque destructivo
	[E.24] Caída del sistema por agotamiento de recursos
	[A.6] Abuso de privilegios de acceso

Cámaras IP	[A.11] Acceso no autorizado
	[A.4] Manipulación de la configuración
	[E.24] Caída del sistema por agotamiento de recursos
Servicios de Soporte externo	[E.19] Fugas de información
	[E.7] Deficiencias en la organización
	[A.29] Extorsión

Tabla 2 Lista general de activos. Fuente: Autor

La vulnerabilidad se considera como una debilidad o carencia de control que podría propiciar la explotación por parte de una o varias amenazas contra un activo. A continuación, en la tabla 3, se detalla las vulnerabilidades de los activos de la organización.

Tipo de activos	**Descripción**	**Vulnerabilidad**
SW	Servidor de Base de datos	Falta de controles de accesos adecuados
		Carencia de mecanismos de integridad de datos
		Información en texto plano
SW	Servidor de Base de datos cloud	Deficiencias en la gestión de autenticación y control de acceso
		Falta de controles de seguridad para prevenir la divulgación no autorizada
		Controles de accesos inadecuados
SW	Servidor Web (Hosting)	Debilidades en el sistema de autenticación y control de accesos
		Falta de medidas y controles de seguridad
		Procesos no estandarizados
SW	Servicio de correos	Correos enviados a receptores erróneos
		Interacción de correos con remitentes de dominios desconocidos
		Falta de Autenticación en el Reenvío de Mensajes
HW	Routers	Uso de Protocolos No Seguros
		Gestión inadecuada de acceso en roles de usuarios
		Falta de Filtrado y Validación de Tráfico
COM	Switches	Uso de Protocolos no seguros
		Gestión inadecuada de acceso en roles de usuarios

		Deficiencias en la infraestructura de comunicaciones
COM	Access Point	Contraseñas Débiles o Predeterminadas
		Configuración Predeterminada no Modificados
		Inadecuada gestión y protección de contraseñas
HW	Laptop	Conexiones a sitios Web no seguros
		Manipulación de los perfiles de usuario
		Fugas de información
HW	PC de escritorio	Respaldo inapropiado o irregular
		Reemplazo inadecuado de equipos con recursos obsoletos
		Manipulación de los perfiles de usuario
HW	Cámaras IP	Configuración Incorrecta
		Configuración Predeterminada no Modificados
		Saturación de ancho de banda
P	Servicios de Soporte externo	Hurto de medios o documentos
		Ausencia de procedimientos y control de cambios
		Divulgación de información

Tabla 3 Matriz de Vulnerabilidades. Fuente: Autor

Para realizar la evaluación cualitativa de los activos, utilizaremos la siguiente escala conforme a lo establecido en la tabla 4.

Escala	Nivel	Representación	Descripción
3	Alta	A	Consecuencias importantes
2	Media	M	Consecuencias de mediana importancia
1	Baja	B	Bajo impacto

Tabla 4 Escala de valoración de los activos de la información. Fuente: Autor

La evaluación otorgada a cada activo se basa en la perspectiva subjetiva de las personas participantes en el proceso, quienes determinarán la importancia de cada activo y, en consecuencia, la necesidad de protegerlo.

Código	Descripción Activos	Valoración
SW	Servidor de Base de datos	A
SW	Servidor de Base de datos cloud	A
SW	Servidor Web (Hosting)	A
SW	Servicio de correos	A
HW	Routers	M
COM	Switches	M
COM	Access Point	M
HW	Laptop	M
HW	PC de escritorio	M
HW	Cámaras IP	M
P	Servicios de Soporte externo	B

Tabla 5 Valoración de los activos de la información. Fuente: Autor

4.3.2. Evaluación de Impacto y la probabilidad

El cálculo del riesgo inherente se refiere al nivel de riesgo antes de que se apliquen medidas de mitigación o controles.

Probabilidad: Se refiere a la medida de la posibilidad de que ocurra un evento no deseado o la materialización de un riesgo.

Impacto: Se refiere a la consecuencias o resultados que pueden surgir si un riesgo se materializa

El criterio de la probabilidad e impacto se ha evaluado utilizando la siguiente escala:

Nivel	Nivel	Representación	Descripción	Frecuencia
3	**Alta**	**A**	Frecuentemente	Al menos 1 vez en el último año
2	**Media**	**M**	Poco Frecuente	Al menos 1 vez en los últimos 2 años
1	**Baja**	**B**	Difícil que ocurra	Al menos 1 vez en los últimos 5 años

Tabla 6 Escala de probabilidad de ocurrencia de una amenaza. Fuente: Autor

Escala	Nivel	Representación	Descripción
3	**Alta**	**A**	Consecuencias importantes
2	**Media**	**M**	Consecuencias de mediana importancia
1	**Baja**	**B**	Bajo impacto

Tabla 7 Escala de impacto. Fuente: Autor

La determinación del cálculo del riesgo es el resultado de la combinación de la probabilidad de que se presente un incidente de seguridad y del impacto que este pueda tener sobre un determinado activo. teniendo en cuenta el giro de negocio de la compañía, así como factores internos y externos que pueden influir en la organización. En este proceso, se han establecido tres niveles.

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3	MODERADO	ALTO	ALTO
	M	2	BAJO	MODERADO	ALTO
	B	1	BAJO	BAJO	MODERADO

Tabla 8 Matriz de Riesgos Fuente: Autor

VALORACIÓN DEL RIESGO	
NIVEL RIESGO	**CALIFICACIÓN**
ALTO	6 a 9
MODERADO	3 a 4
BAJO	1 a 2

Tabla 9 Valoración del riesgo. Fuente: Autor

Mapa de riesgo de los activos

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3		A11,A15,E19	
	M	2			
	B	1			

Tabla 10 Servidor de base de datos Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3		A11,A6,E19	
	M	2			
	B	1			

Tabla 11 Activo: Servidor de base de datos cloud. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3		A24	A11
	M	2	E15		
	B	1			

Tabla 12 Activo: Servidor de base de datos. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3		A5,A9	E19
	M	2			
	B	1			

Tabla 13 Servidor de correos. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3	A24	A11,A6	
	M	2			
	B	1			

Tabla 14 Activo: Routers. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3			I8
	M	2	A11	A6	
	B	1			

Tabla 15 Activo: Switches Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3			
	M	2	E4	A11,A6	
	B	1			

Tabla 16 Activo: Access Points. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3	E25	A11	
	M	2	A6		
	B	1			

Tabla 17 Activo: Laptops. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3			
	M	2	A26,A6	E24	
	B	1			

Tabla 18 Pc de escritorio Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3			
	M	2	A11,A4	E24	
	B	1			

Tabla 19 Activo: Cámaras IP. Fuente: Autor

RIESGO			PROBABILIDAD		
			B	M	A
			1	2	3
IMPACTO	A	3		E19,E7,A29	
	M	2			
	B	1			

Tabla 20 Activo: Servicio de Soporte Externo Matriz de Riesgos. Fuente: Autor

DESCRIPCIÓN	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO	CRITICIDAD
Servidor de Base de datos	[A.11]Acceso no autorizado	2	3	6	ALTO
	[A.15] Modificación deliberada de la información	2	3	6	ALTO
	[E.19] Fugas de información	2	3	6	ALTO
Servidor de Base de datos cloud	[A.11]Acceso no autorizado	2	3	6	ALTO
	[E.19] Fugas de información	2	3	6	ALTO
	[A.6] Abuso de privilegios de acceso	2	3	6	ALTO
Servidor Web (Hosting)	[A.11]Acceso no autorizado	3	3	9	ALTO
	[A.24] Denegación de servicio	2	3	6	ALTO
	[E.15] Alteración accidental de la información	1	2	2	BAJO
Servicio de correos	[E.19] Fugas de información	3	3	9	ALTO
	[A.5] Suplantación de la identidad del usuario	2	3	6	ALTO
	[A.9] [Re-]encaminamiento de mensajes	2	3	6	ALTO
Routers	[A.11]Acceso no autorizado	2	3	6	ALTO
	[A.6] Abuso de privilegios de acceso	2	3	6	ALTO
	[A.24] Denegación de servicio	1	3	3	MODERADO
Switches	[A.11]Acceso no autorizado	1	2	2	BAJO
	[A.6] Abuso de privilegios de acceso	2	2	4	MODERADO
	[I.8] Fallo de servicios de comunicaciones	3	3	9	ALTO
Access Point	[A.11]Acceso no autorizado	2	2	4	MODERADO
	[E.4] Errores de configuración	1	2	2	BAJO
	[A.6] Abuso de privilegios de acceso	2	2	4	MODERADO
Laptop	[A.11]Acceso no autorizado	2	3	6	ALTO
	[A.6] Abuso de privilegios de acceso	1	2	2	BAJO
	[E.25] Pérdida de equipos	1	3	3	MODERADO
PC de escritorio	[A.26] Ataque destructivo	1	2	2	BAJO
	[E.24] Caída del sistema por agotamiento de recurso	2	2	4	MODERADO
	[A.6] Abuso de privilegios de acceso	1	2	2	BAJO
Cámaras IP	[A.11] Acceso no autorizado	1	2	2	BAJO
	[A.4] Manipulación de la configuración	1	2	2	BAJO
	[E.24] Caída del sistema por agotamiento de recurso	2	2	4	MODERADO
Servicios de Soporte externo	[E.19] Fugas de información	2	3	6	ALTO
	[E.7] Deficiencias en la organización	2	3	6	ALTO
	[A.29] Extorsión	2	3	6	ALTO

Tabla 21 Criticidad de los activos Fuente: Autor

4.4. Tratamiento de riesgos

Basándonos en los datos presentados en la Tabla 21, se puedo verificar que los activos con un nivel de riesgo más elevado considerado como alto:

Los valores 1 al 4 son riesgos aceptables para la empresa, los valores entre 6 y 9 son riesgos altos que requieren tener un tratamiento.

Existen varias opciones para el tratamiento del riesgo:

- **Reducción del riesgo**

Se implementan acciones para disminuir la probabilidad o el impacto del riesgo, o ambos; comúnmente implica la aplicación de controles.

- **Aceptación del riesgo**

No se implementa ninguna acción o medidas de tratamiento y los riesgos aceptados deben ser supervisados de manera continua.

- **Evitar el riesgo**

Se prescinde de las acciones que generan el riesgo, lo que implica la decisión de no emprender o detener la actividad que lo origina.

- **Transferir el riesgo**

Se reduce la probabilidad o las consecuencias del riesgo al transferir o compartir una parte de este.

DESCRIPCIÓN	RIESGO	CRITICIDAD	TRATAMIENTO	TIPO DE CONTROL	CONTROLES
Servidor de Base de datos	6	ALTO	Mitigar	Preventivo	A.9.1.1 Política de control de acceso
	6	ALTO	Mitigar	Preventivo	A.9.4.5 Uso de utilidades con privilegios del sistema
	6	ALTO	Evitar	Preventivo	A.9.3.1 Uso de la información secreta de autenticación
Servidor de Base de datos cloud	6	ALTO	Mitigar	Preventivo	A.9.4.1 Restricción del acceso a la información
	6	ALTO	Mitigar	Preventivo	A.9.3.1 Uso de la información secreta de autenticación
	6	ALTO	Mitigar	Preventivo	A.9.2.3 Gestión de privilegios de acceso
Servidor Web (Hosting)	9	ALTO	Mitigar	Preventivo	A.9.4.1 Restricción del acceso a la información
	6	ALTO	Mitigar	Preventivo	A.13.1.1 Controles de red
	2	BAJO	Evitar	Preventivo	A.12.1.2 Gestión de cambios || A.12.4.1 Registro de eventos
Servicio de correos	9	ALTO	Mitigar	Preventivo	A.13.2.3 Mensajería electrónica
	6	ALTO	Mitigar	Preventivo	
	6	ALTO	Mitigar	Preventivo	
Routers	6	ALTO	Mitigar	Preventivo	A.9.1.2 Acceso a las redes y a los servicios de red
	6	ALTO	Mitigar	Preventivo	A.9.2.3 Gestión de privilegios de acceso
	3	MODERADO	Mitigar	Preventivo	A.13.1.1 Controles de red
Switches	2	BAJO	Mitigar	Preventivo	A.9.2.3 Gestión de privilegios de acceso
	4	MODERADO	Evitar	Preventivo	A.9.2.3 Gestión de privilegios de acceso
	9	ALTO	Mitigar	Preventivo	
Access Point	4	MODERADO	Mitigar	Preventivo	A.9.1.2 Acceso a las redes y a los servicios de red
	2	BAJO	Mitigar	Correctivo	
	4	MODERADO	Mitigar	Preventivo	A.9.2.3 Gestión de privilegios de acceso
Laptop	6	ALTO	Mitigar	Preventivo	A.9.1.1 Política de control de acceso
	2	BAJO	Evitar	Preventivo	A.9.2.3 Gestión de privilegios de acceso
	3	MODERADO	Aceptar	Correctivo	A.11.2.6 Seguridad de los equipos fuera de las instalaciones
PC de escritorio	2	BAJO	Transferir	Preventivo	
	4	MODERADO	Transferir	Preventivo	A.11.2.4 Mantenimiento de los equipos
	2	BAJO	Aceptar	Correctivo	A.9.2.3 Gestión de privilegios de acceso
Cámaras IP	2	BAJO	Mitigar	Preventivo	A.9.1.2 Acceso a las redes y a los servicios de red
	2	BAJO	Mitigar	Preventivo	
	4	MODERADO	Aceptar	Correctivo	A.11.2.4 Mantenimiento de los equipos
Servicios de Soporte externo	6	ALTO	Mitigar	Preventivo	A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores A.12.1.1 Documentación de
	6	ALTO	Mitigar	Preventivo	A.16.1.1 Responsabilidades y procedimientos
	6	ALTO	Mitigar	Preventivo	A.9.4.1 Restricción del acceso a la información A.13.2.4 Acuerdos de confidencialidad o no revelación

Tabla 22 Controles. Fuente: Autor

DESCRIPCIÓN	RIESGO	CRITICIDAD	TRATAMIENTO	T. CONTROL	CONTROLES
Servidor de Base de datos	6	ALTO	Mitigar	Preventivo	Herramientas de autenticación multifactor con el objetivo de evitar intentos automatizados, accesos no autorizados mediante contraseñas robadas, ataques de fuerza bruta y el uso indebido de contraseñas reutilizables.
	6	ALTO	Mitigar	Preventivo	Gestionar de manera periódica los privilegios de los usuarios para asegurar un control efectivo. Esto incluye la supervisión continua para prevenir y controlar cualquier acceso no autorizado.
	6	ALTO	Mitigar	Preventivo	Disponer de acuerdos de confidencialidad para proteger la información. Estos acuerdos aseguran que todas las partes involucradas cumplan con sus obligaciones, estableciendo un marco legal y contractual que refuerza la confidencialidad y previene la divulgación no autorizada de información.
Servidor de Base de datos cloud	6	ALTO	Mitigar	Preventivo	Herramientas de autenticación multifactor con el objetivo de evitar intentos automatizados, acceso no autorizado mediante contraseñas robadas, ataques de fuerza bruta y el uso indebido de contraseñas reutilizables.
	6	ALTO	Mitigar	Preventivo	Contar con acuerdos de confidencialidad o no divulgación adaptados a los requisitos específicos de la organización es esencial para prevenir posibles fugas de información. Estos acuerdos establecen claramente las expectativas y obligaciones de las partes involucradas, garantizando un marco legal y contractual que refuerce la confidencialidad y evite la divulgación no autorizada de información sensible.
	6	ALTO	Mitigar	Preventivo	Gestionar de manera periódica los privilegios de los usuarios para asegurar un control efectivo. Esto incluye la supervisión continua para prevenir y controlar cualquier acceso no autorizado.
Servidor Web (Hosting)	9	ALTO	Mitigar	Preventivo	Herramientas de autenticación multifactor con el objetivo de evitar intentos automatizados, acceso no autorizado mediante contraseñas robadas, ataques de fuerza bruta y el uso indebido de contraseñas reutilizables.
	6	ALTO	Mitigar	Preventivo	La implementación de una herramienta de seguridad que monitorea, filtra y analiza el flujo de tráfico desde Internet hacia el servidor web es esencial para gestionar y mitigar los siguientes riesgos de seguridad.
Servicio de correos	9	ALTO	Mitigar	Preventivo	Utilización de herramiemtas cifrado de extremo a extremo para envío de documentos confidenciales mediante correo electrónico. Uso de autenticación multifactor para prevenir intentos automatizados, contrañas robada, ataques de fuerza bruta y uso de contraseñas reutilizables. Uso de Los protocolos seguros para envio/rececpcion de mails ,configurar filtros antispam para reducir la cantidad de correo No Deseados y evitar ser victima de phishing y accesos no autorizados.
	6	ALTO	Mitigar	Preventivo	
	6	ALTO	Mitigar	Preventivo	
Routers	6	ALTO	Mitigar	Preventivo	Realizar una segmentación de red mediante equipos de seguridad con el fin de negar el tráfico proveniente de redes no autorizadas. Además, implementar un control estricto sobre la gestión de privilegios de acceso para fortalecer la seguridad de la red.
	6	ALTO	Mitigar	Preventivo	Gestionar de manera periódica los privilegios de los usuarios para asegurar un control efectivo. Esto incluye la supervisión continua para prevenir y controlar cualquier acceso no autorizado.
Switches	9	ALTO	Mitigar	Preventivo	Utilizar firewalls y sistemas de filtrado para proteger los servicios de comunicación contra amenazas externas y ataques maliciosos.
Laptop	6	ALTO	Mitigar	Preventivo	Utilizar Herramientas de autenticación multifactor con el objetivo de evitar intentos automatizados, acceso no autorizado mediante contraseñas robadas, ataques de fuerza bruta y el uso indebido de contraseñas reutilizables.
Servicios de Soporte externo	6	ALTO	Mitigar	Preventivo	Disponer de acuerdos de confidencialidad o no divulgación que se ajusten a los requisitos específicos de la organización.
	6	ALTO	Mitigar	Preventivo	Implementación de políticas de seguridad de la información, respaldadas por el establecimiento de normativas para la gestión de datos sensibles. Este enfoque se complementa con la asignación de responsabilidades definidas.
	6	ALTO	Mitigar	Preventivo	Implementación de medidas para restringir el acceso a la información, asegurando que únicamente personal autorizado tenga la capacidad de acceder a datos sensibles y críticos. Y mediante el establecimiento de acuerdos formales de confidencialidad o no revelación con el propósito de prevenir situaciones de extorsión, protegiendo así la integridad y confidencialidad de la información sensible de la organización.

Tabla 23 Riegos tratados Fuente: autor

CAPÍTULO 5

DISEÑO DE PROPUESTA DE SEGURIDAD EN CAPAS

5.1. ANALISIS DE SEGMENTACIÓN DE RED

La segmentación de la red funciona como una capa adicional de seguridad en el perímetro al dividir una red en diversos segmentos o subredes. Cada segmento opera como red local independiente brindando a los administradores de redes y sistemas la capacidad de aplicar políticas detalladas y específicas a cada una. Esto posibilita un control preciso del tráfico entre las subredes, proporcionando una visión clara de las interacciones.

El principal objetivo de la segmentación de la red es gestionar el flujo de tráfico de red y restringir el acceso a información confidencial, lo que, a su vez, reduce la superficie de ataque frente a posibles amenazas. Entre las diversas ventajas se tiene:

Fuerte protección de datos: Ayuda a proteger datos sensibles de accesos no autorizados dado que mientras más segmentaciones y controles de tráfico existan en la

red limitara el acceso no autorizado y restringe la propagación de amenazas potenciales dentro de la red.

Contención eficaz de las amenazas: Sí un atacante accede a una red especifica, le tomará tiempo en poder ingresar al resto de redes y de esta manera ayudará a evaluar la amenaza y aumentar la seguridad en los demás equipos de las demás subredes.

Control de acceso limitado: Utilizando políticas de mínimo privilegio para limitar el número de personas que tienen acceso a una determinada red, reduciendo así la posibilidad de que un atacante acceda a la red.

Para lograr tener una buena segmentación de red se debe implementar:

- Vlans
- Subnetting
- Listas de control de acceso (ACL)

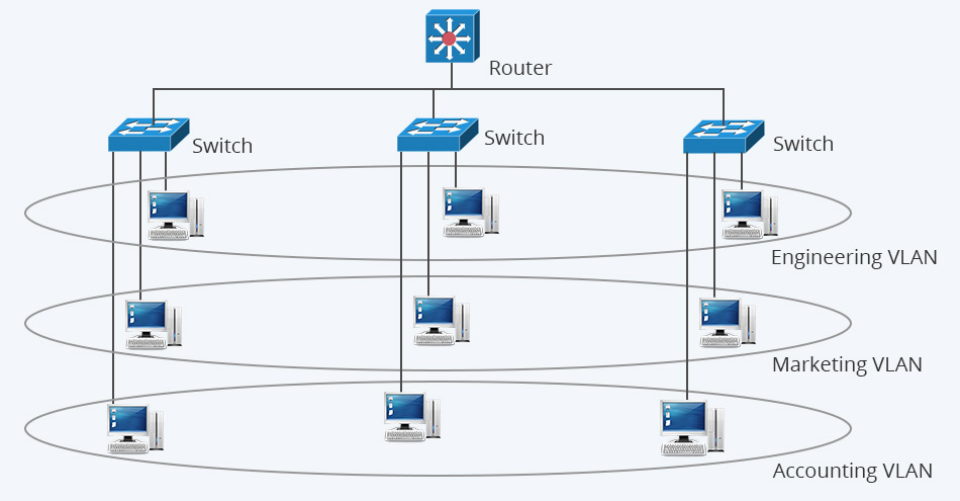


Figura 9 Segmentación por Vlan. redes [20]

5.2. ANÁLISIS DE SISTEMAS DE SEGURIDAD PERIMETRAL

La seguridad perimetral implica establecer los límites del perímetro de una organización para proteger los sistemas contra intrusiones, amenazas o ataques cibernéticos, para evitar que los datos confidenciales se vean comprometidos. Un sistema de seguridad perimetral, además de detectar amenazas, realiza inspecciones y análisis de posibles patrones de ataque en la red. Se instala entre la red externa y la interna, actuando como una barrera de protección en una organización asegurando la disponibilidad, integridad y disponibilidad de la información.

Los Objetivos de la seguridad perimetral son:

Soportar ataques externos.

- Detectar e identificar los ataques recibidos y alertar.
- Segmentar y proteger los sistemas y servicios en función de su superficie de ataque.
- Filtrar y bloquear el tráfico ilegitimo.

Dentro de los componentes de seguridad perimetral se destacan los siguientes:

Firewalls: Equipos de seguridad por los que pasa el tráfico de la red y que aceptan o lo deniegan según políticas o reglas de acceso. Pueden funcionar a nivel de red donde permite o deniega el tráfico en función de la IP de origen y de la IP de destino o a nivel de subredes (conjunto de IPs de origen y de IPs de destino) o a nivel de aplicación permitiendo o denegando el tráfico en función del protocolo utilizado en las comunicaciones (HTTP, HTTPS, DNS, NTP, FTP, SMTP, etc).

Sistema de Detección de Intrusos (IDS): Su funcionalidad es vigilar las intrusiones y notificar un ataque desde dentro de la red. Consiste en uno o varios dispositivos que monitorean la red buscando violaciones de políticas o actividades maliciosas.

Sistema de Prevención de Intrusiones (IPS): Su funcionalidad es detener automáticamente las intrusiones a partir de un listado de reglas predeterminadas. Intercepta el tráfico entrante, bloquea y elimina los datos maliciosos y no requiere de la intervención directa de un administrador.

Sistema anti-DDos: Diseñados para prevenir o mitigar los ataques de denegación de servicio (DoS) o los ataques distribuidos de denegación de servicio (DDoS). Por lo general, estos sistemas requieren un período de aprendizaje para modelar el comportamiento normal y las tendencias del tráfico de la red, estableciendo líneas base para los diferentes volúmenes y tipos de tráfico. Una vez que se activan en modo de bloqueo, son capaces de detectar desviaciones con respecto a estas líneas base durante un ataque, bloqueando o mitigando efectivamente la amenaza y evitando que el tráfico anómalo ingrese a la red.

Antivirus y Antispam: Inspeccionan el correo electrónico de los servidores para filtrar aquellos que tienen contenido malicioso y evitar que entren a la red y lleguen a los destinatarios.

5.3. ANÁLISIS DE GESTIÓN DE IDENTIDADES Y ACCESOS (IAM)

La gestión de identidades y accesos (IAM), garantiza que solamente las personas autorizadas, y nadie más, tengan acceso a los recursos tecnológicos que necesitan para realizar su trabajo. Este sistema Incluye políticas y tecnologías que conforman un proceso que abarca para toda la empresa con la finalidad de identificar, autenticar y autorizar adecuadamente a personas, grupos de personas o aplicaciones de software a través de atributos como los derechos de acceso de los usuarios y las restricciones basadas en sus identidades.

EL sistema de gestión de identidades evita el acceso no autorizado a sistemas y recursos, ayuda a evitar el robo de datos empresariales o protegidos, y genera alertas y alarmas cuando personas o programas no autorizados intentan acceder a estos, ya sea desde dentro o desde fuera del perímetro de la empresa.
Las soluciones de gestión de identidades no solo protegen el acceso al software y los datos, sino que también protegen los recursos de hardware de una empresa, como servidores, redes y dispositivos de almacenamiento, contra accesos no autorizados que pueden desembocar en un ataque de programas de secuestro. La gestión de identidades ha ganado importancia durante la última década debido a la cantidad, cada vez mayor, de exigencias globales de cumplimiento normativo y control, las cuales buscan proteger los datos confidenciales de cualquier tipo de las vulneración [17].

La gestión de identidades se centra en administrar los atributos relacionados con el usuario, grupo de usuarios, dispositivos u otras entidades de la red que necesitan acceder a recursos. También sirve para proteger identidades en una gran variedad de tecnologías de identidad digital, como contraseñas, autenticación multifactor (MFA), inicio de sesión único (SSO) y controles biométricos, entre otras. Normalmente, esto se consigue mediante la adopción de aplicaciones y plataformas de software de gestión de identidades[18] .

La gestión de identidades implica tres conceptos principales: identificación, autorización y autenticación.

Identificación

La identificación es la capacidad de identificar inequívocamente a un usuario, dispositivo o aplicación dentro de la red empresarial en función de sus atributos.

Autenticación

La autenticación es el proceso de verificación de la identidad que se atribuye una entidad de la red en base a sus credenciales. Se pueden utilizar tres factores para la verificación:

- Factor de conocimiento, que se basa en algo que el usuario sabe, como una contraseña o PIN.
- Factor de titularidad, que se basa en un artículo que el usuario tiene, como una tarjeta de identidad, una tarjeta inteligente o un pase de seguridad.
- Factor de inherencia, que se basa en el atributo de un usuario, como las huellas dactilares u otros rasgos biométricos.

Autorización

Consiste en el proceso de otorgar acceso a los recursos de red a una entidad o tipo de usuario específico, de una forma coherente con las políticas y la gobernanza de la empresa. Por ejemplo, otorgar permiso a un usuario para editar un archivo compartido en una red requiere una autorización. En resumen, la autenticación establece la identidad de un usuario y la autorización, qué es lo que puede hacer. Para mantener un entorno de red seguro, la autenticación debe realizarse antes de la autorización.

Un sistema de IAM ideal ayudará a lograr lo siguiente:

- Definir los privilegios de acceso de usuarios a aplicaciones, datos y sistemas.
- Proteger el acceso a las cuentas más importantes por parte de usuarios no autorizados y atacantes maliciosos.

- Obtener una visibilidad total de todas las actividades de los usuarios y los privilegios de acceso.
- Mejorar la experiencia del usuario con un acceso fácil a múltiples aplicaciones y servicios mediante un solo conjunto de credenciales, y así aumentar la productividad.
- Reducir la fatiga de contraseñas, que suele ser la causa de las filtraciones de datos.
- Agregar capas adicionales de seguridad con la autenticación de varios factores.
- Reducir los costos de TI y servicio de asistencia con mecanismos de autoservicio, de modo que los usuarios puedan enviar solicitudes de acceso según su perfil.
- Simplificar las funciones del administrador permitiendo a los administradores gestionar los controles de acceso desde una ubicación central [19].

5.4. ANÁLISIS DE SOLUCIONES DLP

La prevención de pérdida de datos (DLP) sirve para garantizar que los usuarios no envíen información delicada o crítica fuera de la red corporativa. El término describe productos de software que ayudan a un administrador de redes a controlar los datos que los usuarios pueden transferir. Los productos de DLP usan reglas de negocio para clasificar y proteger la información confidencial y crítica, para que los usuarios no autorizados no puedan intercambiar datos de manera accidental o malintencionada, cosa que podría poner en riesgo a la organización. Por ejemplo, si un empleado intenta reenviar un correo electrónico empresarial fuera del dominio corporativo o cargar un

archivo corporativo a un servicio de almacenamiento en la nube para el consumidor, como Dropbox, el empleado no recibirá autorización [20] .

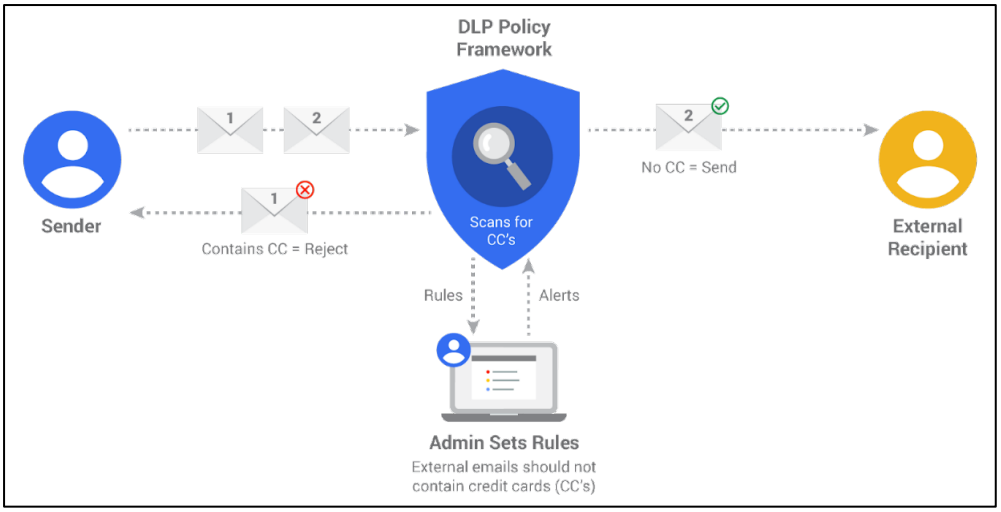


Figura 10 Soluciones DLP [24]

Principales causas de la fuga de datos

Exfiltración: la exfiltración de datos es el acto de robar o transferir datos de forma inadmisible desde un dispositivo o red. Puede ser realizado por personas externas o internas que realizan ciberataques como phishing o ataques DDoS. Los datos que normalmente se extraen incluyen credenciales de inicio de sesión y propiedad intelectual.

Amenazas internas: Las amenazas internas son especialmente peligrosas porque el riesgo proviene del interior de la empresa. Los iniciados incluyen empleados o ex empleados de la empresa, contratistas y socios comerciales. Debido al acceso que tienen los usuarios internos, las amenazas internas dejan los datos confidenciales vulnerables a la explotación.

Exposición de datos involuntaria o negligencia: Las infracciones a menudo ocurren debido a la negligencia de un empleado o, de otra parte. Varias razones pueden contribuir a esto, procedimientos de seguridad deficientes, la implementación inadecuada de programas de capacitación en ciberseguridad o la falta de aplicación del principio de privilegio mínimo. Este principio promueve la personalización de restricciones de acceso a la información confidencial según los roles laborales, minimizando el riesgo de exposición no autorizada.

Funcionamiento de las herramientas DLP

Una solución DLP utiliza una combinación de medidas de ciberseguridad estándar, como firewalls, herramientas de protección de endpoints, servicios de monitoreo y software antivirus, y soluciones avanzadas, como inteligencia artificial (IA), aprendizaje automático (ML) y automatización, para evitar que se produzcan datos. infracciones, detectar actividad anómala y contextualizar la actividad para el equipo de seguridad de la información.

Las tecnologías DLP suelen respaldar una o más de las siguientes actividades de ciberseguridad:

Prevención: establece una revisión en tiempo real de los flujos de datos y restrinja inmediatamente actividades sospechosas o usuarios no autorizados.

Detección: identifica rápidamente actividades anómalas a través de una visibilidad de datos y medidas mejoradas de monitoreo de datos.

Respuesta: Optimiza las actividades de respuesta a incidentes mediante el seguimiento y la notificación del acceso y movimiento de datos en toda la empresa.

Análisis: Contextualiza actividades o comportamientos de alto riesgo para que los equipos de seguridad fortalezcan las medidas de prevención o informen las actividades de remediación.

5.5. DISEÑO DE ARQUITECTURA

A continuación, en la ilustración 8 el diagrama del diseño de la arquitectura de red.

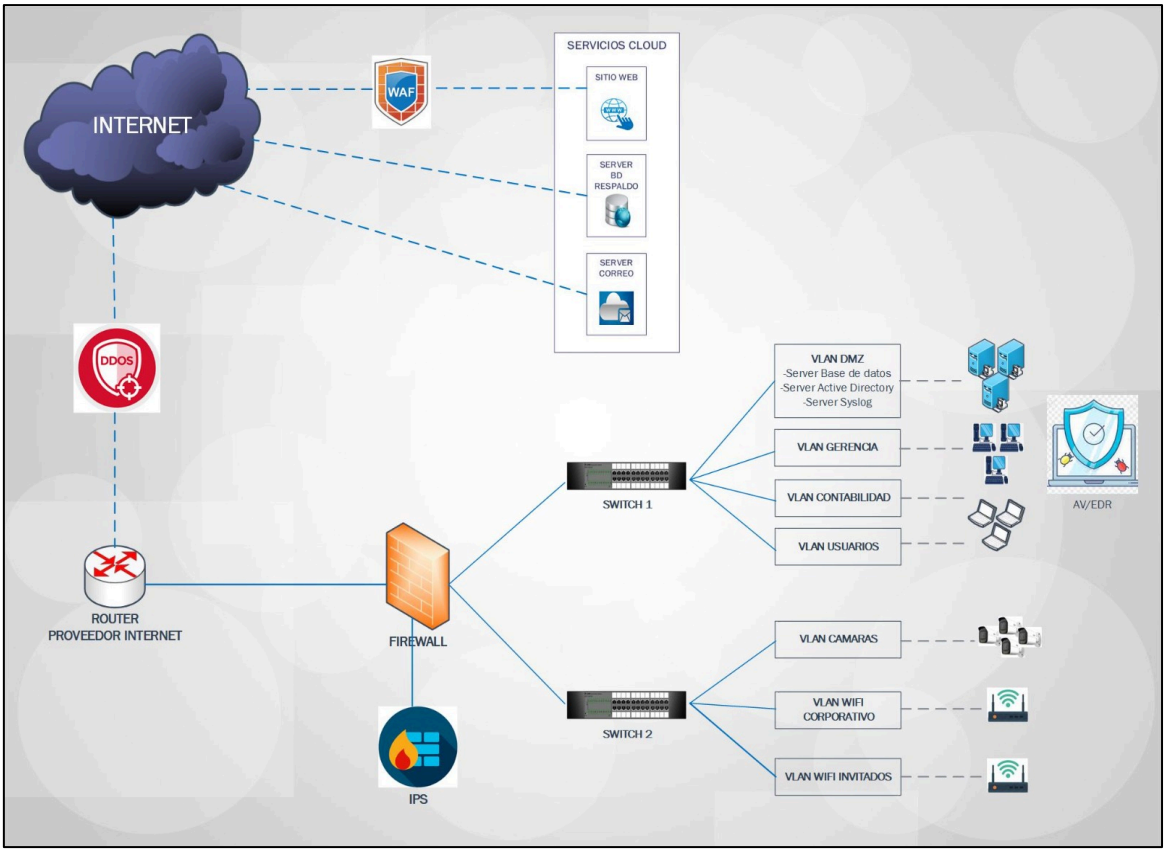


Figura 11 Propuesta de diseño de red. Fuente: Autor

Para asegurar un sistema confiable, es esencial adoptar una estrategia de seguridad integral que integre diversas medidas preventivas, acciones proactivas, así como capacidades de detección y respuesta. El objetivo principal es salvaguardar la integridad, confidencialidad y disponibilidad de la información, proporcionando una

defensa completa y eficaz frente a las amenazas cibernéticas. En caso de que una línea de defensa sea vulnerada, las otras capas están preparadas para prevenir la infiltración de amenazas.

En el diseño de la arquitectura de seguridad propuesta, se han incorporado los siguientes componentes para proteger el núcleo de la organización y reducir la superficie de ataque:

Anti-DDoS:

Proporciona detección y mitigación contra ataques de denegación de servicio distribuido (DDoS) para asegurar la disponibilidad de servicios esenciales.

IPS (Sistema de Prevención de Intrusiones):

Detecta y previene intrusiones, bloqueando activamente amenazas conocidas y comportamientos anómalos. Se integra en la Lan para inspeccionar el tráfico entre VLANs.

Firewall:

Establece políticas de seguridad para controlar y filtrar el tráfico de red, previniendo accesos no autorizados y protegiendo contra amenazas externas.

AV/EDR (Antivirus/Respuesta y Detección de Amenazas Endpoint):

Brinda protección en los dispositivos finales contra malware y amenazas, y realiza un monitoreo continuo de los dispositivos de los usuarios con capacidad de respuesta ante incidentes de seguridad.

WAF (Firewall de Aplicaciones Web):

Garantiza la seguridad del servidor web mediante el análisis de las solicitudes HTTP/HTTPS, examinando cada petición antes de que llegue a la aplicación.

La seguridad en capas que ofrece esta estructura integral se convierte en un pilar fundamental para garantizar que la empresa se encuentre preparada para hacer frente a una amplia gama de amenazas cibernéticas. No solo proporciona una defensa sólida y adaptable, sino que también se destaca por su capacidad para evolucionar y responder de manera ágil frente a posibles brechas o ataques. Esta flexibilidad no solo se traduce en una mayor protección de los activos y datos de la organización, sino que también contribuye significativamente a fortalecer su reputación y confianza en el mercado. En última instancia, esta seguridad en capas no solo se trata de prevenir y proteger, sino también de adaptarse proactivamente al cambiante panorama de ciberseguridad, lo que asegura un entorno empresarial seguro y protegido.

CONCLUSIONES

1. Al analizar el estado actual de la infraestructura y los servicios proporcionados por la empresa en el marco de este estudio, se concluye que existe una notable carencia de seguridad tanto lógica como física en los accesos a los sistemas y áreas de tratamiento de información identificados. Es evidente la necesidad de implementar medidas efectivas para salvaguardar la integridad y confidencialidad de la información crítica de la organización.
2. Tras la revisión del sitio web, se observa que carece de servicios dedicados y herramientas de seguridad que posibiliten el análisis del tráfico web y la detección de posibles amenazas y ataques cibernéticos. Además, durante la validación realizada a través del sitio Mozilla Observatory, Nmap y Nessus, se identificaron deficiencias de seguridad en el código del sitio web. Estas deficiencias representan una potencial amenaza para la seguridad y la integridad de los datos almacenados en el sitio web.
3. Es importante que la empresa realice una inversión en la adquisición de infraestructura y servicios tecnológicos. Esta inversión se enfocará en fortalecer la seguridad de la red interna y externa, así como en obtener un servicio especializado para el portal web. Este enfoque estratégico no solo contribuirá a

la mitigación de riesgos, sino que también respaldará la creación de una infraestructura más resistente y segura. La inversión no solo responde a las necesidades presentes, sino que también proyecta la empresa hacia un futuro digital sólido y confiable.

RECOMENDACIONES

1. Elaborar un plan integral de seguridad como componente esencial donde aborde de manera específica las deficiencias identificadas en el análisis de riesgos, proponiendo soluciones concretas y estratégicas para fortalecer la postura de seguridad de la organización y asegurar la sostenibilidad a largo plazo de su infraestructura y servicios. Este plan debe incluir programas de educación y concientización a los usuarios referentes a la ciberseguridad, con el fin de reforzar las prácticas seguras y reducir los riesgos asociados a errores humanos.
2. Revisar con el proveedor de hosting la migración a una IP pública dedicada para el sitio web. La razón principal radica en que la IP actual se encuentra asociada a varios dominios esto puede ocasionar conflictos de recursos y potenciales vulnerabilidades de seguridad. Por lo tanto, la migración a una IP pública dedicada ofrecería una mayor estabilidad, seguridad y confiabilidad para el funcionamiento del sitio web. Además, se sugiere mejorar el nivel de seguridad del código del sitio web y no exponer puertos no seguros hacia le

internet, lo que permitirá mantener la integridad de los datos y la privacidad de los usuarios.

3. Implementar infraestructura y servicios tecnológicos para fortalecer la seguridad de la red interna y externa especialmente en la seguridad especializada para el portal web. Esta medida no solo aborda las deficiencias actuales identificadas en el análisis del estado actual, sino que también establece la base para un futuro digital robusto y confiable. La inversión en esta área, alineada con una estrategia proactiva, no solo mitiga los riesgos inmediatos, sino que también posiciona a la empresa para enfrentar los desafíos tecnológicos emergentes, garantizando la seguridad y la eficiencia de sus operaciones digitales.

BIBLIOGRAFÍA

[1] «Por qué las pymes deben tomar medidas de seguridad informática». Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://www.eset.com/ec/empresas/compania/por-que-las-pymes-deben-tomar-medidas-de-seguridad-informatica/

[2] A. Pagán y K. Elleithy, «A Multi-Layered Defense Approach to Safeguard Against Ransomware», en *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, ene. 2021, pp. 0942-0947. doi: 10.1109/CCWC51732.2021.9375988.

[3] «Informe e-País: El comercio electrónico en Ecuador». Accedido: 22 de noviembre de 2023. [En línea]. Disponible en: https://www.ivace.es/Internacional_Informes-Publicaciones/Pa%C3%ADses/Ecuador/Ecuadorecommerceicex2020.pdf

[4] A. C. L. Casa, M. L. G. Gavilanez, C. C. C. Caiza, y J. A. C. Moreano, «Importancia de políticas de seguridad Informática de acuerdo a las ISO 27001 para pequeñas y medianas empresas del Ecuador», *Cienc. Ing. Apl.*, vol. 5, n.º 2, Art. n.º 2, ago. 2021.

[5] «Seguridad informática en las PyMES de la ciudad de Quevedo | Journal of business and entrepreneurial studie». Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://journalbusinesses.com/index.php/revista/article/view/97/221

[6] «Reporte: Midiendo el impacto financiero de la seguridad informática en los negocios.» Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://latam.kaspersky.com/blog/reporte-midiendo-el-impacto-financiero-de-la-seguridad-informatica-en-los-negocios/7711/

[7] «Recursos». Accedido: 22 de noviembre de 2023. [En línea]. Disponible en: https://www.iso27000.es/iso27002.html

[8] «Top 7 Ecommerce Security Threats in 2023». Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://cybersecuritynews.com/ecommerce-security-threats/

[9] «Ingeniería social | INCIBE | INCIBE». Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://www.incibe.es/aprendeciberseguridad/ingenieria-social

[10] «Serie 27k». Accedido: 24 de noviembre de 2023. [En línea]. Disponible en: https://www.iso27000.es/iso27000.html

[11] «Arquitectura de seguridad: ¿qué es y por qué es importante?», Saint Leo University. Accedido: 24 de noviembre de 2023. [En línea]. Disponible en: https://worldcampus.saintleo.edu/noticias/que-es-la-arquitectura-de-seguridad-informatica-por-que-es-importante-la-arquitectura-de-seguridad

[12] «¿Qué es un WAF?», Check Point Software ES. Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://www.checkpoint.com/es/cyber-hub/what-is-web-application-firewall/

[13] «Soluciones de prevención, seguridad y protección contra ataques DDoS». Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://es.radware.com/solutions/security/

[14] «Corporate infrastructure protection: Kaspersky Endpoint Detection and Response (EDR) | Kaspersky». Accedido: 24 de noviembre de 2023. [En línea]. Disponible en: https://www.kaspersky.com/enterprise-security/wiki-section/products/kaspersky-endpoint-detection-and-response-edr

[15] «¿Qué es un sistema de detección de intrusos (IDS)?», Check Point Software ES. Accedido: 21 de noviembre de 2023. [En línea]. Disponible en: https://www.checkpoint.com/tw/es/cyber-hub/what-is-an-intrusion-detection-system-ids/

[16] {{ AUTHOR }}, «Mozilla Observatory». Accedido: 23 de enero de 2024. [En línea]. Disponible en: https://observatory.mozilla.org/analyze/proinma.net

[17] «¿Qué es la gestión de identidades? | Glosario de VMware | ES». Accedido: 23 de enero de 2024. [En línea]. Disponible en: https://www.vmware.com/es/topics/glossary/content/identity-management.html

[18] «What is Identity Management? | Glossary». Accedido: 23 de enero de 2024. [En línea]. Disponible en: https://www.hpe.com/lamerica/es/what-is/identity-management.html

[19] «¿Qué es la gestión de identidad y acceso? | Zoho Vault», Zoho. Accedido: 23 de enero de 2024. [En línea]. Disponible en: https://www.zoho.com/es-xl/vault/identity-and-access-management-iam.html

[20] «DLP - ¿Qué es la prevención de pérdida de datos? | Proofpoint ES», Proofpoint. Accedido: 23 de enero de 2024. [En línea]. Disponible en: https://www.proofpoint.com/es/threat-reference/dlp