ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

PROPUESTA DE UN PLAN DE SEGURIDAD PARA PREVENIR LAS VULNERABILIDADES EN LA PLATAFORMA INFORMÁTICA DEL CUERPO DE BOMBEROS, GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SANTO DOMINGO, EMPLEANDO LAS NORMAS ISO 27001

ÁLVARO HUMBERTO PINANGO BAYAS

Trabajo de Titulación modalidad: Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

Riobamba - Ecuador
Enero 2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, determinado: "PROPUESTA DE UN PLAN DE SEGURIDAD PARA PREVENIR LAS VULNERABILIDADES EN LA PLATAFORMA INFORMÁTICA DEL CUERPO DE BOMBEROS, GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SANTO DOMINGO, EMPLEANDO LAS NORMAS ISO 27001", de responsabilidad del señor Álvaro Humberto Pinango Bayas, ha sido prolijamente revisada y se autoriza su presentación.

Tribunal:

Ing. Luis Eduardo Hidalgo Almeida, PhD
PRESIDENTE

LUIS EDUARDO HIDALGO ALMEIDA
Firmado digitalmente por LUIS EDUARDO HIDALGO ALMEIDA
Nombre de reconocimiento (DN): c=EC, o=BANCO CENTRAL DEL ECUADOR, ou=ENTIDAD DE CERTIFICACION DE INFORMACION-ECIBCE, l=QUITO, serialNumber=0000445780, cn=LUIS EDUARDO HIDALGO ALMEIDA
Fecha: 2021.01.26 09:49:15 -05'00'

Ing. Pablo Martí Méndez Naranjo, Mag.
DIRECTOR

PABLO MARTI MENDEZ NARANJO
Firmado digitalmente por PABLO MARTI MENDEZ NARANJO
Nombre de reconocimiento (DN): c=EC, o=SECURITY DATA S.A. 1, ou=ENTIDAD DE CERTIFICACION DE INFORMACION, serialNumber=160920175409, cn=PABLO MARTI MENDEZ NARANJO
Fecha: 2021.01.26 10:17:24 -05'00'

Ing. Danilo Geovanny Barreno Naranjo, Mag.
MIEMBRO

DANILO GEOVANNY BARRENO NARANJO
Firmado digitalmente por DANILO GEOVANNY BARRENO NARANJO
Fecha: 2021.01.26 10:48:44 -05'00'

Ing. Diego Gustavo Caiza Méndez, Mag.
MIEMBRO

Firmado electrónicamente por:
DIEGO GUSTAVO CAIZA MENDEZ

Riobamba, enero 2021

DERECHOS INTELECTUALES

Yo, Álvaro Pinango Bayas, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
ALVARO HUMBERTO PINANGO BAYAS

_____

Álvaro Pinango Bayas
C.C.: 1721953188

DECLARACIÓN DE AUTENTICIDAD

Yo, Álvaro Pinango Bayas, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Firmado electrónicamente por:
ALVARO HUMBERTO PINANGO BAYAS

Álvaro Pinango Bayas
C.C.: 1721953188

DEDICATORIA

A mis padres.

Álvaro Pinango B.

AGRADECIMIENTO

A mis padres.

Álvaro Pinango B.

TABLA DE CONTENIDO

CAPÍTULO III

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

LISTADO DE ANEXOS

RESUMEN

El objetivo fue proponer un plan de seguridad para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo, empleando las normas ISO 27001, para lo cual, se realizaron pruebas de penetración a dicha plataforma informática para la detección de vulnerabilidades, mientras que, se implementó un plan de seguridad basado en políticas de seguridad de la norma ISO 27001 para su prevención. La detección de vulnerabilidades se basó en 8 de los 10 riesgos de seguridad enmarcados en OWASP Top 10-2017, utilizando como herramientas de escaneo y explotación a Nessus, Vega, BurpSuite y Zenmap, Kali Linux (metasploit), lo que permitió identificar fallas de seguridad como: inyección de código malicioso, pérdida de autenticación, exposición de datos sensibles, pérdida de control de acceso, control de seguridad incorrecta, uso de componentes con vulnerabilidades conocidas y registro y monitoreo insuficientes; es decir se determinó que la plataforma informática presentó todos las 8 vulnerabilidades establecidas, por lo tanto, se concluyó que la plataforma era 100% vulnerable , motivo por el cual se creó el plan de seguridad con directrices de mejora acorde a las vulnerabilidades encontradas, mismo que fue implementado por un periodo de prueba de dos meses, dando como resultado una mejora significativa en el nivel de seguridad, reduciendo de 8 a 2 las vulnerabilidades existentes en dicha plataforma, dando como resultado de la implementación del plan se seguridad una mejora del 75% en la seguridad de la plataforma informática de la institución. Es por ello que, se recomienda seguir implementando políticas de seguridad para generar una cultura preventiva en los funcionarios y así seguir evitando situaciones de riesgo.

Palabras Clave: <SEGURIDAD TELEMÁTICA>, <PLAN DE SEGURIDAD>, <VULNERABILIDADES>, <PENTESTING>, <POLITICAS DE SEGURIDAD>

ABSTRACT

The objective for this research work was to propose a security plan to prevent vulnerabilities in the computer platform of the Fire Department of the Municipal GAD of Santo Domingo, using the ISO 27001 standards, for which, penetration tests were carried out on said computer platform for the detection of vulnerabilities, while a security plan based on security policies of the ISO 27001 standard was implemented for their prevention. The vulnerability detection was based on 8 of the 10 security risks outlined in OWASP Top 10-2017, using Nessus, Vega, BurpSuite and Zenmap, Kali Linux (metasploit) as scanning and exploitation tools, which allowed identifying flaws of security such as: malicious code injection, loss of authentication, exposure of sensitive data, loss of access control, improper security control, use of components with known vulnerabilities and insufficient registration and monitoring; It was determined that computer platform presented all 8 established vulnerabilities, therefore, it was concluded that the platform was 100% vulnerable, which is why the security plan was created with improvement guidelines according to the vulnerabilities found, same which was implemented for a trial period of two months, resulting in a significant improvement in the level of security, reducing the existing vulnerabilities in said platform from 8 to 2, resulting in the implementation of the security plan an improvement of 75 % in the security of the institution's computer platform. That is recommended to continue implementing security policies to generate a preventive culture in employees and thus continue to avoid risk situations.

Keywords: <TELEMATIC SECURITY>, <SECURITY PLAN>, VULNERABILITIES>, <PENTESTING>, <SECURITY POLICIES>

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Antecedentes

La constante evolución de la tecnología ha logrado que las empresas se sientan seguras de migrar sus servicios a la Internet. Esta migración se ha conseguido implementando servicios web, los mismos que al disponer de fácil accesibilidad se encuentran expuestos ante vulnerabilidades de seguridad que muchas veces los mismos desarrolladores desconocen; estas pueden llegar a ser descubiertas y utilizadas por terceros con el fin de tomar el control de los sistemas y obtener acceso al activo más valioso de las organizaciones, la información; por lo tanto, la implementación de seguridades a nivel de hardware y software, así como los lineamientos para el buen uso de los recursos son importantes.

Las plataformas informáticas, son el conjunto de hardware y software que permiten dar lugar a sistemas complejos que proveen facilidades a las organizaciones, permitiendo la accesibilidad, interoperabilidad y la globalización de la información en un solo punto de acceso disponible.

Con el crecimiento de nuevas plataformas informáticas han surgido nuevas vulnerabilidades de seguridad que las acechan, motivo de ello hace que los desarrolladores no solo se preocupen hoy en día por el funcionamiento y la agilidad de los servicios, sino también, deben buscar la manera de brindar la seguridad necesaria para evitar que dichas plataformas caigan a terceros por desconocimiento del tema.

El CB-GADM-SD (Cuerpo de Bomberos del GAD Municipal de Santo Domingo) al ser una institución pública que almacena información delicada de otras entidades, tiene un compromiso legal y económico ante diferentes estamentos públicos por el no cumplimiento de procesos puedan intentar vulnerar los sistemas y manipularlo a su favor, con la finalidad de evitar pagos y sanciones que describen las diferentes leyes ecuatorianas.

Debido a que no se han realizado trabajos que consideren lineamientos para mitigar las vulnerabilidades en la plataforma informática, se presenta este trabajo donde se propone un plan de seguridad capaz de prevenir las vulnerabilidades existentes; tomando en cuenta la seguridad de la información, seguridad relativa a los recursos humanos, control de acceso, seguridad física

y del entorno, seguridad de las comunicaciones, gestión de incidentes de seguridad de la información y su respectivo cumplimiento.

1.2. Planteamiento del problema

1.2.1. Situación problemática

El desconocimiento de normas y políticas mínimas de seguridad por parte del personal responsable del desarrollo, implementación y mantenimiento de plataformas web, ha dado paso al desarrollo del presente caso de estudio.

Partiendo de la amplia aceptación de nuevas tecnologías de la información (TI) en las organizaciones, hasta llegar a la completa sistematización de sus procesos y a su vez originando una constante dependencia de las mejores prácticas para salvaguardar el bien más preciado por las organizaciones, la información. Las vulnerabilidades de seguridad y el deseo de usuarios malintencionados, hacen que la seguridad de dicha información esté propensa a los ataques generados por terceros, los mismos que aprovechan la falta de lineamientos de seguridad para vulnerar los servicios y tomar control de ellos.

Uno de los mecanismos para la sistematización de procesos y gestión de información son las plataformas informáticas, dentro de las cuales los principales métodos son la implementación de plataformas con arquitectura cliente-servidor, permitiendo concentrar la información en un punto específico y que los usuarios puedan acceder a esta desde distintos puntos.

El presente proyecto de investigación propone un plan de seguridad para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo empleando las normas ISO 27001, dicho plan se basará en procedimientos y lineamientos necesarios para reducir significativamente el problema de esta investigación.

1.2.2. Formulación del problema

¿Se disminuirán las vulnerabilidades al aplicar un plan de seguridad en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo empleando las normas ISO 27001?

1.2.3. Sistematización del problema

- ¿Cuáles son las vulnerabilidades más comunes en la plataforma informática?

- ¿Cómo establecer los procedimientos para prevenir y mitigar vulnerabilidades de la plataforma informática al emplear la norma ISO 27001?

- ¿Existirá una mejor seguridad de la plataforma informática del CB-GADM-SD al implementar el plan de seguridad?

- ¿El personal técnico conoce las medidas de prevención a posibles ataques?

- ¿El personal técnico conoce sobre las políticas de seguridad existentes en su organización?

1.3. Justificación de la investigación

1.3.1. Justificación teórica

La seguridad informática nace en vista que la información se ve afectada por muchos factores ajenos a nuestro control, es una disciplina, donde su objetivo es mantener el conocimiento, los datos y la información fuera del alcance de eventos no planeados, tales como: el robo, espionaje, daños, amenazas y otros peligros. La seguridad de la información incluye todas las acciones tomadas con anticipación y para prevenir dichas amenazas, los desarrolladores deben aplicar las mejores prácticas de codificación, realizar revisiones de seguridad del código, pentesting (pruebas de penetración), utilizar analizadores de vulnerabilidad de códigos, entre otros (Wang, Gong, Chen, Sun, & Yang, 2013, p. 78).

El Cuerpo de Bomberos del GAD Municipal de Santo Domingo al tratar de brindar un mejor servicio a la ciudadanía ha implementado una plataforma informática en la cual permite a los usuarios acceder a sus servicios desde cualquier dispositivo con acceso a internet, merced de ello, es necesario realizar un escaneo de vulnerabilidades para identificar las amenazas que pueden llegar a perjudicar su correcto desempeño y poder llegar a su prevención.

Al implementar este plan de seguridad los desarrolladores de la institución, así como personal encargado de la administración de los equipos y la red contarán con los lineamientos suficientes para prevenir la aparición de nuevas vulnerabilidades en la plataforma informática.

1.3.2. Justificación metodológica

El objetivo de un análisis de vulnerabilidades es descubrir debilidades de seguridad y rendimiento que pueden afectar y comprometer la confidencialidad, integridad y disponibilidad de la información de sistemas de información. Actualmente, existen normas, modelos y estándares para

implementar programas y controles para la mitigación de riesgos, por ejemplo: las normas ISO 27001, ITIL, COBIT y estándares del NIST (Cuevas et al., 2018, p. 1035).

La parte investigativa de este trabajo se basa en las normas ISO 27001 para la mitigación de vulnerabilidades mediante la creación de un plan de seguridad que permita salvaguardar la confidencialidad, integridad y disponibilidad de la información de la plataforma informática de la presente investigación.

1.3.3. Justificación práctica

Al implementar un plan de seguridad capaz de detectar las vulnerabilidades e implementar recomendaciones con las normas necesarias que la alta dirección sea capaz de aplicar; de esta manera prevenir la exposición a eventos no controlados y así asegurar a la ciudadanía en general que serán los beneficiarios directos, puesto que su información se encontrará protegida y resguardada bajo aplicaciones que establecen políticas seguras.

Para lograr una adecuada protección de los sistemas de información, los datos y la información, es necesaria la intervención de todo el personal de la organización. Además, las acciones deben encontrarse enmarcadas en un proceso lógico, sistemático, documentado y que pueda ser difundido internamente para garantizar la gestión correcta de la seguridad informática y de la información, siguiendo el ciclo de mejora continua (Solarte, Rosero, & Benavides, 2015, p. 497).

Para la medición del nivel de seguridad se establece OWASP, utilizando uno de sus proyectos como es el Top 10, esta herramienta permite en la investigación establecer las 10 vulnerabilidades más críticas en aplicaciones web, las cuales serán evaluadas para obtener el nivel de seguridad de la aplicación. Del mismo modo, el análisis de herramientas y los casos de estudio se realizan mediante pruebas de penetración a la plataforma informática en el ambiente de producción.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Proponer un plan de seguridad para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo empleando las normas ISO 27001.

1.4.2. Objetivos específicos

- Establecer las vulnerabilidades más comunes en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo.

- Elaborar un plan de seguridad que brinde los lineamientos necesarios para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo empleando las normas ISO 27001.

- Verificar el nivel de seguridad implementando el plan propuesto para la plataforma informática.

1.5. Planteamiento de la hipótesis

La implementación del plan de seguridad propuesto mejorará el nivel de seguridad de la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo

CAPÍTULO II

2. MARCO DE REFERENCIA

2.1. Antecedentes del problema

Con el fin de brindar legitimidad y hacer comprensible este estudio para los lectores, se han analizado varios trabajos de investigación similares de los cuales se ha encontrado temas que defienden y sirven de referentes para el desarrollo de esta investigación.

El estudio de Solarte, con el tema: "Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001" (2015, p. 498), en la que se concluye lo siguiente:

- Del proceso llevado a cabo, se puede concluir que no existe una cultura de seguridad de la información dentro de las organizaciones, tampoco existen sistemas de control de seguridad informática, y mucho menos, procesos y procedimientos documentados para protección de la información (Solarte et al., 2015, p. 498).

- El resultado del estudio realizado mostró que es imperativo el apoyo y compromiso real de la gerencia o administración para el proceso de diseño, implementación e implantación de un SGSI de acuerdo a los resultados de la auditoria; además, se deben formalizar los procesos y procedimientos que así lo requieran y documentarlos; también considera que se debe implementar un sistema de control de seguridad informático estableciendo mecanismos que permitan la medición permanente orientadas hacia la mejora de la seguridad de la información y al diseño en cada una de las organizaciones de acuerdo a la necesidad que surja en las organizaciones (Solarte et al., 2015, p. 498).

Del mismo modo, mediante estudio de (Amado Ballen, Ayala Calderón, & Sierra Morales, 2017, p. 36), con el tema: "Análisis de vulnerabilidades en aplicaciones WEB desarrolladas en PHP versión 5.6.24 con Base de Datos MySQL versión 5.0.11 a partir de ataques SQL Inyección", en la que se concluye lo siguiente:

- El campo de inyecciones SQL contiene numerosas técnicas de defensa (Anup Shakya, 2011, 56), sin embargo, no significa que sea el ataque menos vulnerable en las aplicaciones web. La

herramienta de la OWASP “Zed Attack Proxy” de uso gratuito detectó algunos agujeros en la seguridad del aplicativo creado para el proyecto, identificando cada uno de ellos, no obstante, no se detectaron vulnerabilidades para ataques de SQL inyección a razón que el framework utilizado tiene funciones pre-establecidas evitando esta técnica, pero se encontraron otras vulnerabilidades como son Application Error Disclosure, X-frameOptions Header NotSet, Cross-Domain JavaScript, Password Autocomplete, Private Ip Disclosure, Web Browser XSS, X-Content-Type-Options (Amado Ballen et al., 2017, p. 37).

- Entre las recomendaciones que presenta este estudio (Amado Ballen et al., 2017, p. 37), se da a conocer el uso de frameworks para el desarrollo de aplicaciones, así como también del constante uso de herramientas para el monitoreo de vulnerabilidades antes y después del lanzamiento de las aplicaciones web con la finalidad de mantener una base de datos de vulnerabilidades siempre actualizada y una aplicación robusta capaz de resistir al ataque mal intencionado de terceros.

En 2015, Hernández y Mejía en su estudio realizado “Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web” mencionan lo siguiente:

> La mejor manera para prevenir las amenazas informáticas en los servidores es actuar de una forma anticipada, detectando las vulnerabilidades más graves, ya que con esto se disminuye la probabilidad de éxito que tendrán los atacantes, para ello realizó un trabajo en el cual examina distintas técnicas y herramientas utilizadas en la actualidad para detectar vulnerabilidades más peligrosas tomando como base las vulnerabilidades las descritas en el OWAS Top 10, generando una matriz de trazabilidad entre ataques, vulnerabilidades, técnicas y herramientas que determinarán cuales vulnerabilidades y ataques pueden ser mitigados con la utilización de dichas técnicas y herramientas (Hernández Saucedo, Ana Laura; Mejia Miranda, 2015, p. 5).

La falta de procedimientos para el aseguramiento de la información en las plataformas informáticas es un problema que va en aumento, esto se debe a que con el paso del tiempo van apareciendo herramientas de fácil acceso que permiten realizar ataques que vulneran fácilmente plataformas informáticas que no mantienen una adecuada configuración en base a lineamientos o estándares previamente establecidos, además, el incremento de los atacantes crece junto con dichas herramientas y por descuido de los administradores de dichas plataformas.

En la publicación de Gómez, se da a conocer una clasificación de cuáles son los principales ataques que presentan los sistemas informáticos, junto con las consecuencias de estos a los sistemas víctimas. De esta manera redacta el rol y la clasificación de los intrusos informáticos en

las redes: hackers, crackers, sniffers, phreakers, spammers, etc. También relata cuales pueden ser las principales motivaciones para realizar ataques, mostrando sus fases prestando especial atención a lo que se ha dado en llamar como el "Triángulo de la Intrusión" para analizar la posibilidad de éxito de un ataque informático, y describir sus principales etapas (2019, p. 1).

Con el fin de evaluar los niveles de seguridad de los sistemas informáticos nace el pentesting, llamado también pruebas de penetración, es un concepto sencillo que va más allá de una serie de pruebas al evaluar las vulnerabilidades identificadas para verificar si las mismas son reales o un falso positivo. Por ejemplo, una auditoría o una evaluación pueden utilizar herramientas de escaneo que proporcionan las vulnerabilidades posibles en múltiples sistemas; por lo tanto, el objetivo de una prueba de penetración es atacar las vulnerabilidades de la misma manera que un usuario malintencionado podría hacerlo para comprobar qué vulnerabilidades son genuinas, reduciendo así la lista real de vulnerabilidades de un sistema (Muniz & Lakhani, 2013, p. 215).

Dirigir el ataque a un solo objetivo revela más sobre su seguridad y tiempo de respuesta para manejar incidentes que un ataque con múltiples objetivos. Al elegir estratégicamente los objetivos, el probador de penetración puede determinar toda la infraestructura de seguridad y el riesgo asociado para una verdadera victima (Muniz & Lakhani, 2013, p. 215). El pentesting evalúa la efectividad de la seguridad existente. Por lo tanto, si un cliente no tiene una seguridad sólida, recibirá poco valor de los servicios de pruebas de penetración.

Muniz y Lakhani, como consultores recomiendan que, los servicios de pruebas de penetración se ofrezcan como un medio para verificar la seguridad de los sistemas existentes una vez que un cliente cree que ha agotado todos los esfuerzos para asegurarlos y está listo para evaluar si existen vacíos existentes en su seguridad (Muniz & Lakhani, 2013, p. 8).

Por lo anteriormente estudiado es que en el presente estudio se pretende brindar un plan de seguridad que ayude a mejor la seguridad de los servicios ofrecidos en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo, aplicando las pruebas de penetración (pentesting) en base a OWASP Top 10 2017 en conjunto con la norma ISO 27001, con el fin de prevenir las vulnerabilidades que pudieran llegar a afectar la calidad del servicio ofrecido por esta entidad, prevenir que usuarios internos y externos tengan acceso no autorizado a la información y además, la unidad de sistemas contará con directrices para realizar una adecuada gestión de la plataforma informática de la que son responsables, puesto que a la presente fecha de elaboración de este proyecto no se cuenta con la respectiva documentación.

2.2. Bases teóricas

2.2.1. Plataformas informáticas

Una plataforma informática es una potente herramienta de gestión empresarial conformada por un conjunto de hardware, software, estándares internacionales, metodologías, servicios y mucho más (Prosultra Consultores, 2017). Algunos ejemplos son: el sistema operativo de un equipo, software base para ejecución de aplicaciones, lenguajes de programación, librerías en tiempo de ejecución, consolas de videojuegos, etc.

2.2.2. Servicios web

Los servicios web son aplicaciones que utilizan protocolos estándares de comunicación y registro para conectarse con otras de manera dinámica, utilizan un formato estándar como XML o una de sus variantes para presentar información y datos, un registro para encontrar servicios ofrecidos por otras aplicaciones, negocian como recibir y enviar información (WSDL), y se adhieren a protocolos de comunicación (SOAP) para enviar la información por internet (HTTP).

Por otro lado, se define también a un servicio web como "el conjunto de aplicaciones o tecnologías con capacidad para interoperar en la Web" (Lapuente & Lapuente, 2013).

Castillo (2018), en una de sus publicaciones hace mención a los beneficios de los servidores web:

- **Promueven la interoperabilidad:** La interacción entre un proveedor y un solicitante de servicio está diseñada para que sea completamente independiente de la plataforma y el lenguaje. Esta interacción requiere un documento WSDL para definir la interfaz y describir el servicio, junto con un protocolo de red (generalmente HTTP).

- **Permiten la integración "justo-a-tiempo":** El proceso de descubrimiento se ejecuta dinámicamente, a medida que los solicitantes de servicio utilizan a los agentes para encontrar proveedores de servicio. Una vez el solicitante y el proveedor de servicio se han ubicado, se utiliza el documento WSDL del proveedor para enlazar al solicitante con el servicio. Esto significa que los solicitantes, los proveedores y los agentes actúan en conjunto para crear sistemas que son auto-configurables, adaptativos y robustos.

- **Reducen la complejidad por medio del encapsulamiento:** Los solicitantes y los proveedores del servicio se preocupan por las interfaces necesarias para interactuar. Como resultado, un solicitante de servicio no sabe cómo fue implementado el servicio por parte del proveedor, y éste a su vez, no sabe cómo utiliza el cliente el servicio. Estos

detalles se encapsulan en los solicitantes y proveedores. El encapsulamiento es crucial para reducir la complejidad.

- **Dan una "nueva vida" a las aplicaciones de legado:** Es relativamente correcto tomar una aplicación, generar un wrapper SOAP, luego generar un documento WSDL para moldear la aplicación como un servicio web.

- **Abren la puerta a nuevas oportunidades de negocio:** Los servicios web facilitan la interacción con socios de negocios, al poder compartir servicios internos con un alto grado de integración.

- **Disminuyen el tiempo de desarrollo de las aplicaciones:** Pues gracias a la filosofía de orientación a objetos utilizada, el desarrollo se convierte más bien en una labor de composición.

2.2.3. Vulnerabilidad, amenazas y riesgo

Los conceptos de vulnerabilidad, amenaza y riesgo se encuentran estrechamente relacionados entre sí aportando las bases para la seguridad en distintos ámbitos como lo es en seguridad informática y de la información (Solarte et al., 2015, p. 499). En esta investigación se tomará las vulnerabilidades como las debilidades del sistema o activo informático en cuanto a seguridad, las amenazas son los posibles ataques que puede hacer una persona (interna o externa) aprovechando las vulnerabilidades, y los riesgos como las diversas maneras en que se presenta la amenaza y la posibilidad de que ese ataque llegue a presentarse en una organización específica.

2.2.3.1 Vulnerabilidad informática

Son fallos de diseño que permite que una amenaza pueda afectar a un recurso. Si se habla de recursos informáticos se suele decir que una vulnerabilidad es un fallo de diseño de un sistema, un sistema no actualizado o un sistema mal configurado que permite que un agente externo, acceda sin permisos apropiados a la información que dicho sistema gestiona, en función del tipo de recurso al que se orienta existen distintas fuentes de información dónde se puede buscar vulnerabilidades aplicables a los sistemas con que se cuenta (Romero Castro et al., 2018, p. 175).

2.2.3.2 Amenazas informáticas

Son consideradas como los ataques realizados a los sistemas informáticos, que pueden o no ocasionar daños a la infraestructura tecnológica, a los sistemas de información o a la información. Las amenazas pueden presentarse por acciones criminales en las que intervienen seres humanos

violando las normas y las leyes, sucesos de orden físico por eventos naturales que se pueden presentar, o aquellos eventos en los que el ser humano propicia las condiciones para determinar un hecho físico, decisiones o acciones que pueden presentar algunas personas por desconocimiento, falta de capacitación y/o abuso de autoridad (Solarte et al., 2015, p. 498).

Las amenazas a los sistemas de información están latentes cada que se interactúa con ellos, al utilizar dispositivos de almacenamiento externos, al ingresar a sitios web, por la inconformidad de empleados insatisfechos dentro de la misma organización, etc. De acuerdo a lo anterior las amenazas pueden ser de varios tipos, entre ellas tenemos las amenazas por intercepción, modificación, interrupción o generación (Solarte et al., 2015, p. 499).

Las amenazas según su origen se clasifican de la siguiente manera:

- **Accidentales:** Son los que son ocasionados por accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes en los sistemas operativos o en el software, errores humanos (Aguilera Lopez, 2010, p. 85).

- **Intencionadas:** Son debidas siempre a la atención humana, como la introducción de software malicioso (aunque este penetre en el sistema por algún procedimiento automático, su origen es siempre humano), intrusión informática, robos o hurtos. Las amenazas intencionadas pueden tener origen en el exterior de la organización o incluso en el personal de la misma (Aguilera Lopez, 2010, p. 85).

2.2.3.3 Riesgos informáticos

Son problemas potenciales, que pueden afectar a los sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento, por lo tanto, los riesgos se pueden clasificar en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura (Solarte et al., 2015, p. 499).

2.2.4. Ataques

Un ataque accidental o deliberado se genera cuando se ha materializado una amenaza (Aguilera Lopez, 2010, p. 85); estos ataques se clasifican según el impacto causado en los activos:

- **Activo:** Si suprimen, dañan, cambian o agregan información, o bien bloquean o saturan los canales de información.

- **Pasivo:** Solamente acceden sin autorización a los datos contenidos en el sistema. Estos son más fáciles de detectar.

Un ataque puede ser directo o indirecto, si se produce desde el atacante al elemento victima directamente, o a través de recursos o personas intermediarias (Aguilera Lopez, 2010, p. 86).

2.2.5. Tipos de intrusos informáticos

- **Hackers:** Son individuos que se dedican a programar ya sea como un pasatiempo o reto técnico para superar un problema, poner a prueba su inteligencia y conocimientos de los acertijos que presenta la Internet. Sin embargo, pueden llegar a tener acceso a información confidencial, es por ello que en varios países esta actividad se está considerando como un delito (Gómez Vieites, 2019, p. 10; Zabala, 2017).

- **Crakes (Blackhats):** Son aquellas personas que fragmentan o quebrantan algún sistema de seguridad de los sistemas informáticos, para obtener beneficios o causar algún daño a la organización, cuya motivación son de interés económico, político, religioso, etc. (Gómez Vieites, 2019, p. 10; Zabala, 2017).

- **Sniffers:** Son los que se dedican a rastrear, intentar recomponer y descifrar los mensajes que circulan por las redes de ordenadores como internet.

- **Phreakers:** Se especializan en investigar y sabotear los sistemas telefónicos, utilizando tecnologías para manipular sus sistemas y obtener beneficios. Ej. realizar llamadas gratuitas. Desarrollan las famosas “cajas azules”, que ocasionan anomalías en las líneas telefónicas. En la actualidad estos tienen como objetivo a la telefonía móvil, a las tecnologías inalámbricas y el VoIP (Gómez Vieites, 2019, p. 10; Zabala, 2017).

- **Spammers:** Una o un grupo de personas que se dedican a enviar e-mails masivos no solicitados con el fin de ocasionar un colapso en los servidores y la sobrecarga de los buzones de los usuarios. Además, estos pueden contener virus informáticos o formar parte de estafas masivas (Gómez Vieites, 2019, p. 10; Zabala, 2017).

- **Piratas informáticos:** Son especialistas en el pirateo de programas y contenidos digitales, infringiendo la legislación sobre la propiedad intelectual, esto lo realizan por negocio la reproducción, apropiación y distribución a gran escala diversos contenidos como software, videos, música, etc. (Gómez Vieites, 2019, p. 10; Zabala, 2017).

- **Creadores de virus y programas dañinos:** son aquellos que se dedican a crear programas y distribuirlos por Internet para conseguir una propagación exponencial, esto lo utilizan para tener acceso a datos sensibles como números de cuentas bancarias y de tarjetas de crédito (Gómez Vieites, 2019, p. 11; Zabala, 2017).

- **Amenazas por personal interno:** Estos pueden realizar amenazas informáticas a la organización de manera voluntaria o involuntaria.

- **Ex-empleados:** Pueden llegar a ser los atacantes más potenciales, puesto que pueden llegar a actuar por despecho o venganza hacia su antigua organización o empresa accediendo a su información una vez conocida la manera o método del manejo de la información (Gómez Vieites, 2019, p. 11; Zabala, 2017).

2.2.6. Penetration Testing, Pentesting

Las pruebas de penetración son la metodología, el proceso y los procedimientos utilizados dentro de pautas específicas y aprobadas para intentar eludir las protecciones de seguridad de un sistema de información. Este tipo de pruebas están asociadas con la evaluación de los ajustes y controles técnicos, administrativos y operativos de un sistema (Broad & Bindner, 2013, p. 114). Las pruebas de penetración solo evalúan la seguridad del sistema de información en el tiempo de desarrollo, por lo que comúnmente a futuro no se realiza una constate evaluación de nuevas pruebas de penetración para medir el nivel de seguridad de una plataforma.

Por lo tanto, su objetivo específico es la prueba finaliza cuando se alcanza el objetivo, es decir, cuando se logra vulnerar las fallas de seguridad o se logra obtener información de suma importancia para hacer uso de ella en un futuro, también finaliza cuando el tiempo disponible para esta prueba se ha agotado (De Jimenez, 2017, p. 3).

2.2.6.1 Tipos de pentest

Existen dos tipos de pentest que se clasifican según el rol que adopta el pentester durante la prueba de penetración:

- **Auditoría Externa (Covert pentest)**: También llamada auditoría de caja negra, pretende valorar el grado de seguridad de la red externa de una organización; es decir, el pentester asume el rol de un atacante externo, que, sin ninguna información previa, puede obtener algún beneficio de la organización, o incluso, acceso a información sensible que comprometa la privacidad de la empresa, consiguiendo de este modo, poner a prueba el

estado de las barreras de seguridad que dispone la empresa entre internet y su red corporativa (Guillen Zafra, 2017, p. 5).

- **Auditoría interna (Overt pentest):** En esta auditoría se pretende valorar el grado de seguridad del entorno privado de una organización; es decir, el pentester asume el rol de un atacante que dispone de acceso a la red interna de la organización (Guillen Zafra, 2017, p. 5). La auditoría interna puede ser de dos tipos, dependiendo de los permisos que tenga el pentester:

    - **Auditoría de caja blanca:** El pentester recibe gran cantidad de información del sistema que va a auditar como puede ser la topología de red, rangos de IP, sistemas operativos, etc. Lo que se pretende es ahorrarle la fase de recolección de información y facilitarle en gran medida la tarea de intrusión para ver si es capaz de encontrar vulnerabilidades en el sistema (Guillen Zafra, 2017, p. 5).

    - **Auditoria de caja gris:** Se combinan los enfoques de caja blanca y caja negra. De esta forma, el pentester asume un rol de usuario sin privilegios dentro de la organización y la cantidad de información que recibe es meramente orientativa (Guillen Zafra, 2017, p. 5).

2.2.6.2 Etapas de un pentesting

Del mismo modo, el pentesting puede ser definido como el estudio de las vulnerabilidades presentes en un sistema objetivo, debidamente autorizado por el propietario de los sistemas y por lo tanto legal, este estudio concluirá con un informe de la situación actual, junto con pruebas de explotación que evalúen la exposición real del sistema objetivo (Gimeno, 2019, p. 14).

Este proceso sigue una metodología que permite dividir el proceso en una serie de fases más pequeñas (Gimeno, 2019, p. 14). En general, el pentesting se dividen en las siguientes etapas:

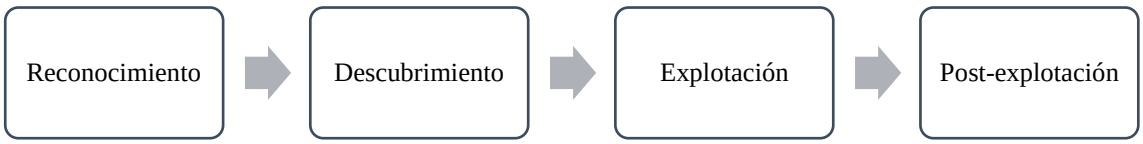


Figura 1-2. **Etapas del pentesting**
Fuente: José & Gimeno, 2019

- **Reconocimiento:** Consiste en la recogida de información, footprinting pasivo u OSINT (Open Source Intelligence). Se le denomina reconocimiento pasivo, porque las tareas que se realizan en ningún momento son intrusivas frente a la infraestructura al objetivo de la

recolección de la información, por lo que no suele ser detectada por los sistemas de seguridad de la organización (Gimeno, 2019, p. 15). La información que se recolecta proviene de fuentes públicas disponibles, es decir, el footprinting recoge información del objetivo a través de todos los directorios de información existentes o mediante diversas técnicas de ingeniería social. Esta etapa es el punto donde más información se debe recoger y sobre la que se realizarán los análisis posteriores (Gimeno, 2019, p. 15).

- **Descubrimiento:** Recoge la información directamente de la infraestructura de la empresa, por lo que sí puede ser detectado por los sistemas de seguridad. El objetivo es recolectar y explorar la infraestructura objetivo, así como un análisis de vulnerabilidades (Gimeno, 2019, p. 16).

- **Explotación:** Es una etapa intrusiva y hace uso de la información obtenida en las fases anteriores, así como las vulnerabilidades descubiertas para realizar un ataque, y conseguir acceso al objetivo. El éxito de la explotación dependerá de la calidad de la información obtenida en las etapas anteriores, así como de la identificación de las vulnerabilidades encontradas en el objetivo planteado (Gimeno, 2019, p. 17).

- **Post-explotación:** El objetivo es seguir explotando un sistema al que ya tenemos acceso, es decir mantener disponible el acceso conseguido, para lo cual se necesita ganar privilegios de alto nivel, penetrar en una subred interna (pivoting), cubrir rastros (en la medida que sea posible evitar que el ataque sea detectado y mantener disponibilidad del acceso al objetivo) (Gimeno, 2019, p. 18).

En la tabla que se presenta a continuación se detalla las características de cada una de las etapas del pentesting en cuanto a su nivel de intrusión y detectabilidad.

Tabla 1-2. Detalle de las etapas del pentesting

Etapa	Denominación	Nivel de Intrusión	Detectable
1	Reconocimiento	PASIVO	NO
2	Escaneo	ACTIVO	SI
3	Explotación	ACTIVO	SI
4	Post-explotación	ACTIVO	SI

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

2.2.6.3 Herramientas para el escaneo y explotación de vulnerabilidades

2.2.6.3.1 Kali Linux

Kali Linux es una nueva distribución de código abierto que facilita las pruebas de penetración, se creó desde cero en Debian y cumple con FHS (estándar de jerarquía del sistema de archivos). Los repositorios de software mejorados sincronizados con los repositorios de Debian hacen que sea más fácil mantenerlo actualizado, aplicar parches y agregar nuevas herramientas. Kali Linux también se puede personalizar fácilmente para que solo contenga los paquetes y las características que se requieren. El entorno de escritorio también se puede personalizar para usar GNOME, KDE, LXDE o lo que prefiera (Sonu Tiwary, 2013, p. 1).

Kali Linux contiene una serie de herramientas que se pueden usar durante el proceso de prueba de penetración. Las herramientas de prueba de penetración incluidas en Kali Linux se pueden clasificar en las siguientes categorías:

- **Recopilación de información:** Presenta varias herramientas que se pueden utilizar para recopilar información sobre DNS, IDS / IPS, escaneo de red, sistemas operativos, enrutamiento, SSL, SMB, VPN, voz sobre IP, SNMP, direcciones de correo electrónico y VPN (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 2).

- **Evaluación de vulnerabilidad:** Aquí existen herramientas para escanear vulnerabilidades, evaluar la red de Cisco y herramientas para evaluar la vulnerabilidad en varios servidores de bases de datos, también incluye herramientas fuzzing (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 2).

- **Aplicaciones web:** Esta categoría contiene herramientas relacionadas con aplicaciones web, como el escáner del sistema de gestión de contenido, la explotación de bases de datos, los fuzzers de aplicaciones web, servidores proxy de aplicaciones web y los escáneres de vulnerabilidades web (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 2).

- **Ataques de contraseña:** En esta categoría, encontrará varias herramientas que se pueden utilizar para realizar ataques de contraseña, en línea o sin conexión (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 3).

- **Herramientas de explotación:** Esta categoría contiene herramientas que pueden utilizarse para explotar las vulnerabilidades encontradas en el entorno de destino. Puede encontrar herramientas de explotación para la red, la Web y la base de datos. También

hay herramientas para realizar ataques de ingeniería social y conocer la información de explotación (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 3).

- **Detección y suplantación:** Las herramientas de esta categoría se pueden utilizar para detectar la red y el tráfico web. Esta categoría también incluye herramientas de suplantación de red como Ettercap y Yersinia (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 3).

- **Mantener el acceso:** Las herramientas de esta categoría podrán ayudar a mantener el acceso a la máquina víctima. Es posible que necesite obtener el nivel de privilegio más alto en la máquina antes de poder instalar herramientas en esta categoría. Aquí, puede encontrar herramientas para backdooring el sistema operativo y aplicaciones web, herramientas para hacer túneles (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 3).

- **Herramientas de informes:** en esta categoría, encontrará herramientas que lo ayudarán a documentar el proceso y los resultados de las pruebas de penetración (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 4).

- **Servicios del sistema:** Esta categoría contiene varios servicios que pueden ser útiles durante la tarea de prueba de penetración, como el servicio Apache, el servicio MySQL, el servicio SSH y el servicio Metasploit (Ali, Shakeel; Allen, Lee; Heriyanto, 2014, p. 4).

2.2.6.3.2 Metasploit

Metasploit es un proyecto de código abierto que ayuda a investigar las vulnerabilidades de seguridad, es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team. Red Team es el equipo ofensivo o encargado del hacking ético, que hace pruebas de intrusión (Rizaldos, 2018).

Rizaldos, en uno de sus webinars del 2018 trató sobre las principales características de mestasploit, las mismas que se listan a continuación:

- Es una herramienta muy completa que tiene muchos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos llamados payloads, que son los códigos que explotan estas vulnerabilidades.

- Dispone de módulos, como los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

- Permite interactuar también con herramientas externas, como Nmap o Nessus.

- Es multiplataforma, algunas versiones ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.

2.2.6.3.3 Nessus

Es un programa de escaneo de vulnerabilidades multiplataforma con interfaz gráfica. Escanea el objetivo, mientras que el cliente muestra el avance e informa sobre el estado de los escaneos (Castillo et al., 2018, p. 1). Se seleccionó Nessus debido a que es una herramienta de evaluación de seguridad, además, cuenta con unas características detalladas a continuación:

- Referencia mundial, porque tiene la mayor base instalada y una mejor experiencia en industria, Nessus ofrece a los clientes la, capacidad de identificar sus mayores amenazas y responder rápidamente.

- Tiene paneles de mando detallados para ayudar a los clientes a fortalecer las redes contra las amenazas cibernéticas.

2.2.6.3.4 *Vega*

Un escáner de Vulnerabilidades de código abierto para probar la seguridad de sitios/aplicaciones web, en la cual nos puede ayudar a encontrar y validar las Inyecciones SQL, Cross-Site Scripting (XSS), Shell Injection, Local File Inclusion, Integer Overflow, entre otras vulnerabilidades (Castillo et al., 2018, p. 1).

2.2.6.3.5 *BurpSuite*

Es una colección de herramientas integradas en una única suite que permite realizar pruebas de seguridad en aplicaciones web, desde el mapeo inicial y el análisis de la superficie hasta la búsqueda y explotación de vulnerabilidades de seguridad. Su principal característica es que puede actuar como un proxy de intercepción, e interceptar el tráfico entre un navegador y un servidor web (Thongthua & Ngamsuriyaroj, 2016, p. 18).

2.2.6.3.6 Zenmap (Nmap)

Su objetivo es proporcionar funciones avanzadas para usuarios experimentados de Nmap (Nmap, 2017). Entre las principales ventajas de esta herramienta está el poder guardar perfiles de escaneos para facilitar su ejecución repetida, además de guardar los resultados de los escaneos, y compararlos a futuro para ver cómo difieren, finalmente es capaz de proporcionar un bosquejo de

la red en la que se trabaja, así como los saltos que se tiene para llegar a un objetivo y la latencia generada en las etapas realizadas.

2.2.7. Análisis de vulnerabilidades

Es un proceso mediante el cual la organización determina el nivel de exposición y la predisposición a la pérdida de elementos ante una amenaza específica (Santo Orcero & Amazon, 2017, p. 35). Un análisis de vulnerabilidades comúnmente se realiza con la finalidad de identificar, mitigar y prevenir la aparición de nuevas debilidades de seguridad.

2.2.8. Análisis de riesgos

Es la actividad que más tiempo llevará en la implantación de un sistema de gestión, y a la que más atención hay que prestarle. Para desarrollar correctamente un análisis de riesgos es importante seguir los siguientes pasos: Establecer los criterios, Identificar los riesgos, probabilidad e impacto y evaluar los riesgos (ISO 27000, 2018a).

2.2.9. Seguridad informática y de la información

2.2.9.1 Seguridad informática

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la organización, protege la confidencialidad, integridad y disponibilidad de la información almacenada en un sistema informático contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesto (Ramos Saky, 2006, p. 25).

Representa al conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y recursos que permiten almacenar y que circule la información que contiene (ACISSI, 2018).

Entre los principales objetivos se pueden destacar los siguientes:

- Minimizar y gestionar los riesgos y detectan los posibles problemas y amenazad a la seguridad.
- Garantizar la adecuada utilización de los recursos y de las aplicaciones del sistema.
- Limitar las pérdidas y conseguir l adecuada recuperación del sistema en caso de un incidente de seguridad.

- Cumplir con el marco legal y con los requisitos impuestos por los clientes en sus contratos (Gómez Vieites, 2019, p. 13).

Para cumplir con estos objetivos una organización debe complementar cuatro planos de actuación:

- Técnico: tanto a nivel físico como a nivel lógico.
- Legal: algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad para el cumplimiento del marco legal vigente y de igual manera realizar las debidas certificaciones basadas en una serie de estándares internacionales (BS77799-2, ISO 27001) o nacionales.
- Humano: sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del personal.
- Organizativo: definición e implementación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación (Gómez Vieites, 2019, p. 13).

2.2.9.2 Ciberseguridad

Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno (Duque Valencia, 2010, p. 4).

2.2.9.3 Seguridad de la información

Según ISO 27000, la seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Según ISO 27000, la seguridad de la información consiste en la aplicación y gestión de los controles apropiados que implica la consideración de una amplia gama de amenazas, con el objetivo de garantizar el éxito comercial sostenido y continuidad, y reducir al mínimo las consecuencias de los incidentes de seguridad de la información. Se logra mediante la aplicación de un conjunto de aplica controles, seleccionados a través del proceso de gestión de riesgos y gestionarse a través de un SGSI, incluidas las políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información (ISO/IEC 27000 et al., 2018).

2.2.10. ISO 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por la Organización Internacional de Normalización (ISO) que es una federación mundial de organismos nacionales de normalización. ISO27000 es un trabajo de preparación de Normas Internacionales llevada a cabo normalmente a través de comités técnicos de ISO. Las organizaciones internacionales, gubernamentales y no gubernamentales también colaboran con su desarrollo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todas las materias de normalización electrotécnica (ISO/IEC 27000 et al., 2018).

Proporciona términos y definiciones que se utilizan comúnmente en la familia de normas de SGSI. Este documento es aplicable a todo tipo y tamaño de la organización de tipo público o privada, grande o pequeña (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) (ISO/IEC 27000 et al., 2018).

2.2.11. ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO), en ella se describe cómo gestionar la seguridad de la información en una organización. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2 (ISO 27000, 2018a).

En este documento se especifican los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI) formalizado en el contexto de los riesgos de negocio globales de la organización. Además, especifica los requisitos para la aplicación de controles de seguridad de la información a medida de las necesidades de las organizaciones (ISO/IEC 27000 et al., 2018).

Cualquier organización puede hacer uso de esta norma, puesto que está redactada por los mejores especialistas del mundo en el tema y proporciona un plan de seguridad para implementar la gestión de seguridad de la información en una organización (ISO 27000, 2018a).

La norma ISO 27001 tiene como objetivo central proteger la confidencialidad, integridad y disponibilidad de la información de la organización. Esto lo realiza mediante la evaluación de los riesgos para luego definir lo que se hará para mitigar o tratar los riesgos encontrados (Advisera, 2019). La filosofía de esta norma se basa en la gestión de riesgos; por lo tanto, se centra en investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Figura 2-2. **Estructura de ISO 27001**
Fuente: Advisera, 2019

Los controles que se van a implementar se presentan bajo la forma de políticas, procedimientos e implementación técnica. Sin embargo, en la mayoría de los casos, la empresa ya tiene el hardware y software, pero no utilizan de una forma segura; por lo que, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales necesarias para prevenir violaciones de seguridad (Advisera, 2019).

Por lo tanto, la gestión de la seguridad de la información no se limita a la seguridad de TI, sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc. (ISO 27000, 2018b).

Existen 4 ventajas esenciales que una organización puede obtener con la implementación de esta norma para la seguridad de la información:

- **Cumplir con los requerimientos legales:** Esta norma proporciona una metodología perfecta para cumplir con las leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información.

- **Obtener una ventaja comercial:** Al obtener la certificación, se mejora la perspectiva frente a otras organizaciones que no la han obtenido, esto mejora significativamente la visión que los demás tienen de la empresa u organización.

- **Menores costos:** Siempre se trata de evitar que se produzcan incidentes de seguridad, ya sea grande o pequeño, puesto que genera la pérdida de dinero; por lo tanto, evitando que la organización genere incidentes se va a ahorrar recursos monetariamente.

- **Una mejor organización:** Existen organizaciones que no tienen tiempo para definir sus procesos y procedimientos; por lo cual, muchas veces el personal desconoce las funciones

que debe cumplir. La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que exige a las entidades escribir sus principales procesos, esto permite reducir el tiempo perdido de sus empleados.

2.2.11.1 Estructura de la norma

- **Introducción:** Describe el proceso para tratar satisfactoriamente los riesgos a los que está expuesta la información
- **Alcance:** Se especifica los requisitos del SGSI adecuados para cualquier tipo de organización.
- **Normativas de referencia:** estable que es esencial para los usuarios de esta norma ISO/IEC27000
- **Términos y definiciones:** se debe consultar el ISO/IEC27000
- **Contexto de la organización:** La Sección 4.4 establece muy claramente que "La organización debe establecer, implementar, mantener y mejorar continuamente" el SGSI.
- **Liderazgo:** La alta dirección debe demostrar liderazgo y compromiso con el SGSI, imponer políticas y asignar funciones, responsabilidades y autoridades de seguridad de la información.
- **Planificación:** Describe el proceso para identificar, analizar y planificar el tratamiento de los riesgos de la información y aclarar los objetivos de seguridad de la información.
- **Apoyo:** Se deben asignar recursos adecuados y competentes, crear conciencia, preparar y controlar la documentación.
- **Operación:** Se detalla sobre la evaluación, el tratamiento de los riesgos de la información, la gestión de cambios y la documentación.
- **Evaluación del rendimiento:** Se debe supervisar, medir, analizar y evaluar (auditar)los controles de la seguridad de la información, los procesos y el sistema de gestión.
- **Mejora:** Abordar los resultados de la auditoría y realizar mejoras continuas.

2.2.11.2 Sistema de Información de Gestión de Seguridad –SGSI

Se compone de las políticas, procedimientos, pautas, recursos y actividades asociadas, gestionadas colectivamente por una organización, en la búsqueda de la protección de sus activos y de la información. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Se basa en una evaluación del riesgo y los niveles de aceptación de la organización diseñada para tratar y mejorar los riesgos de manera efectiva. El análisis de los requisitos para la protección de los activos y la aplicación de controles adecuados para garantizar su protección, según sea necesario, contribuye a la implementación exitosa de un SGSI (ISO/IEC 27000 et al., 2018). Los siguientes principios fundamentales también contribuyen a la implementación exitosa de un SGSI:

- Tener conciencia de la necesidad de seguridad de la información;
- La asignación de responsabilidades para la seguridad de la información;
- La incorporación de compromiso de la dirección y de los intereses de todas las partes;
- El aumento de los valores sociales;
- Evaluaciones de riesgo que determinan los controles apropiados para alcanzar niveles aceptables de riesgo;
- La seguridad incorporada como un elemento esencial de las redes y sistemas de información;
- La prevención activa y detección de incidentes de seguridad de la información;
- Garantizar un enfoque integral de la gestión de seguridad de la información;
- Realizar una reevaluación continua de la seguridad de la información y haciendo de las modificaciones apropiadas.

2.2.11.3 Formas de afrontar los riesgos

Una vez realizado el análisis, se debe definir un plan de tratamiento o esquema de mejora, en el que se tengan en cuenta las distintas consecuencias potenciales de esos riesgos, estableciendo una criticidad para cada uno de ellos y así poder evaluar con objetividad las diferentes amenazas.

- **Eliminar el riego:** Si el riesgo es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, ésta debe poner todos los medios para tratar de eliminarlo, de manera que haya una posibilidad cero de que la amenaza se llegue realmente a producir (ISO Tools, 2019).

- **Mitigarlo:** En la gran mayoría de ocasiones no es posible llegar a la eliminación total del riesgo. Cuando esto sucede la organización puede aceptar el riego, ser consciente de que la amenaza para la información existe y dedicarse a monitorearlo con el fin de controlarlo. Definitivamente, se trata de implantar las medidas preventivas o correctivas necesarias con el fin de reducir la posibilidad de ocurrencia o el impacto de riesgo (ISO Tools, 2019).

- **Trasladarlo:** Esta opción está relacionada con la contratación de algún tipo de seguro que compense las consecuencias económicas de una pérdida o deterioro de la información. Sea cual sea el plan de tratamiento elegido por la organización, la gestión de riesgos debe garantizar a la organización la tranquilidad de tener suficientemente identificados los riesgos y los controles pertinentes, lo cual le va a permitir actuar con eficacia ante una eventual materialización de los mismos (ISO Tools, 2019).

2.2.12. OWASP

La implementación de la seguridad en aplicación al momento de su desarrollo es un tema fundamental a considera, sin embargo, muchas veces este aspecto es dejado a un lado y no se lo toma en cuenta. A raíz de esto surgen sinnúmero de fallos de seguridad en las aplicaciones, las mismas que llegan a comprometer la integridad de su información, llegando incluso a provocar pérdidas importantes tanto de información como financieras. Por lo tanto, es necesario disponer de medios de referencia sobre la seguridad en aplicaciones, fallos de seguridad a los que están expuestas, así como herramientas que permitan obtener información de las vulnerabilidades que los asechan; con el objetivo de solventar estas y otras necesidades nace OWASP.

OWASP es una comunidad en línea enfocada a desarrollar proyectos abiertos internacionales relacionados con la seguridad de aplicaciones web. Su misión es hacer que la seguridad dentro de las aplicaciones sea más visible y así poder tomar decisiones sobre conceptos de seguridad basándose en información verídica y contrastada. Es importante destacar que cualquiera puede participar en OWASP y que todos sus proyectos, materiales, documentación y productos son libres y de código abierto (OWASP, 2019, p. 1).

2.2.12.1 Valores de OWASP

Como organización, el desarrollo y futuro de OWASP también se rige bajo una serie de valores:

- **Transparencia:** Todo lo relativo a la organización es transparente, desde sus finanzas hasta el código fuente de sus proyectos pueden ser consultadas directamente desde su sitio web y desde los repositorios de código respectivamente (OWASP, 2019).

- **Innovación:** Promueven y favorecen la experimentación para aquellas soluciones a los nuevos desafíos de seguridad que aparecen.

- **Global:** Cualquier persona de cualquier parte del mundo está invitada a participar en la comunidad de OWASP, pudiendo aplicar su admisión desde un formulario.

- **Integridad:** Se declaran como una comunidad honesta y en la que se puede confiar. También se declaran neutrales sobre el aspecto comercial de los productos de seguridad disponibles en el mercado, no posicionándose sobre alguno de ellos (OWASP, 2019).

2.2.12.2 Integración con otras normas

El objetivo con el que se creó esta comunidad fue para desarrollar aplicaciones web seguras. La mayoría de estos proyectos tienen documentos, guías y herramientas que pueden ser útiles para una implementación de ISO 27001. Pero, ¿por qué es tan útil OWASP para ISO 27001? Porque el objetivo principal de ISO 27001 es la protección de la información y durante el desarrollo del software, eso también es importante. Además, un gran número de empresas no saben cómo proteger la información durante el desarrollo de software y OWASP puede ser una gran herramienta para eso (Segovia, 2018).

2.2.12.2.1 Alcance y estructura

OWASP se centra en las aplicaciones web, principalmente porque hoy en día casi todo está en línea: tiendas, supermercados, programas de televisión, agencias de viajes, bibliotecas, etc. La mayoría de las aplicaciones están codificadas para la web, y OWASP da soporte a los desarrolladores a crear un código seguro dándoles muchas herramientas para los procesos de desarrollo de software. Este proyecto se compone de los siguientes tipos de proyectos:

- Proyectos emblemáticos (proyectos maduros)

- Proyectos de laboratorio (proyectos de nivel medio y aún en funcionamiento)

- Proyectos de incubadora (nuevos proyectos)

Para una implementación de ISO 27001, los proyectos más interesantes son los proyectos emblemáticos, puesto que son proyectos terminados y estables. Estos son proyectos maduros, y sus recursos (documentación, herramientas, etc.) son utilizados por empresas de todo el mundo.

2.2.12.2.2 ISO 27001 y desarrollo de software

ISO 27001 tiene un anexo donde puede encontrar 114 controles de seguridad. Estos controles son genéricos, aunque todos tienen el mismo objetivo: la protección de la información. Por lo tanto, puede ver los controles relacionados con recursos humanos, cumplimiento, proveedores, TI, etc. A continuación, se describe brevemente los controles relacionados con el desarrollo de software:

- **A.14.2.1 Política de desarrollo seguro:** Están relacionados con la definición de reglas para el desarrollo de software. Por ejemplo, una regla puede ser evitar variables globales o evitar algunas funciones inseguras durante la codificación.

- **A.14.2.4 Restricciones a los cambios en los paquetes de software**: Están relacionados con los cambios en los paquetes de software. Por ejemplo, debe tener cuidado con los cambios en un proyecto de código abierto y las herramientas a implementar.

- **A.14.2.5 Principios de ingeniería de sistemas seguros**: Están relacionados con los principios básicos de ingeniería de sistemas seguros.

- **A.14.2.6 Entorno de desarrollo seguro**: Se refiere a la protección del entorno de desarrollo. Por ejemplo, solo los desarrolladores pueden acceder al entorno de desarrollo, cada desarrollador cuenta con un usuario único, el entorno de desarrollo está aislado, etc.

- **A.14.2.8 Pruebas de seguridad del sistema**: Están relacionados con la prueba de la funcionalidad de seguridad del sistema. Por ejemplo, si ha definido un canal seguro para acceder a una aplicación web, debe verificar si el https está en su lugar durante el acceso.

- **A.14.2.9 Pruebas de aceptación del sistema**: Están relacionados con el desempeño de algunas pruebas antes de aceptar el sistema. Por ejemplo, puede usar herramientas de análisis de código o escáneres de vulnerabilidades, y puede decidir no aceptar un sistema si tiene vulnerabilidades críticas.

2.2.12.3 Proyectos para seguridad de la información

Los mejores proyectos OWASP para la seguridad de la información, más interesantes para ISO 27001 se describen en la siguiente sección:

- **OWASP Top 10:** Define un top 10 de los riesgos de seguridad de aplicaciones web más críticos. Esto puede ayudarnos a definir una política de desarrollo segura y definir principios de ingeniería de sistemas seguros relacionados con el control A.14.2.1. Según este proyecto se puede definir una política de desarrollo segura para evitar

vulnerabilidades técnicas (Ej. Cross-Site Scripting (XSS), inyección de código malicioso, etc.). También está relacionado con el control A.14.2.5, porque permite definir principios básicos relacionados con los principios de ingeniería segura.

- **Proyecto estándar de verificación de seguridad de aplicaciones**: Ayuda a probar la seguridad de la aplicación y del sistema, que está relacionada con el control A.14.2.8. Este proyecto proporciona la documentación específica para definir los requisitos para probar los controles técnicos de seguridad de las aplicaciones web. Ej: este proyecto define los requisitos para probar la arquitectura, la autenticación, el control de acceso, etc.

- **OWTF (marco de prueba web ofensivo):** Ayuda a realizar pruebas de escaneo de vulnerabilidad, que está relacionado con el control A.14.2.9. Este proyecto brinda una herramienta de software para realizar piratería ética.

- **Proyecto de entorno de prueba web**: Ayuda a definir un entorno de desarrollo seguro, que está relacionado con el control A.14.2.6. Brinda herramientas de software para establecer un entorno de prueba independiente.

Por lo tanto, se puede combinar ISO 27001 y OWASP para obtener los mejores resultados en el desarrollo de software y en la prevención de vulnerabilidades en plataformas informáticas.

ISO 27001 es una solución global para la seguridad de la información, está compuesta por controles de seguridad genéricos, mientras que OWASP es una solución específica para prevenir vulnerabilidades en aplicaciones web. Ambas son compatibles y pueden trabajar juntas para la protección de la información. ISO 27001 puede ser usada de forma global en la administración de seguridad de la información, y OWASP puede ser la mejor opción para problemas específicos de seguridad relacionados con el desarrollo de software (Segovia, 2018).

2.2.12.4 OWASP Top 10

OWASP Top 10 es un poderoso documento de conciencia, el cual representa un amplio consenso sobre los riesgos de seguridad más críticos para aplicaciones web. Los miembros del proyecto incluyen una variedad de expertos en seguridad de todo el mundo que han compartido su experiencia para producir esta lista (OWASP, 2017, p. 2).

Fox (2006) en su publicación menciona que OWASP Top 10 es un documento de conocimiento estándar para los desarrolladores y seguridad de aplicaciones web, además, representa un amplio consenso sobre los riesgos de seguridad más críticos que pueden perjudicar el funcionamiento de

las dichas aplicaciones. Cuando las organizaciones adoptan este documento e inician sus procedimientos garantizan que sus aplicaciones web minimicen estos riesgos.

Uno de sus principales objetivos es educar a los desarrolladores, diseñadores, arquitectos, gerentes y organizaciones sobre las consecuencias de las debilidades más comunes y más importantes de la seguridad de las aplicaciones web. El Top 10 proporciona técnicas básicas para protegerse contra estas áreas con problemas de alto riesgo, y proporciona la orientación para continuar desde allí (OWASP, 2017, p. 3).

A continuación, se describen los 10 principales riesgos de seguridad de las aplicaciones web según la clasificación del Top 10 de OWASP en la actualización de 2017:

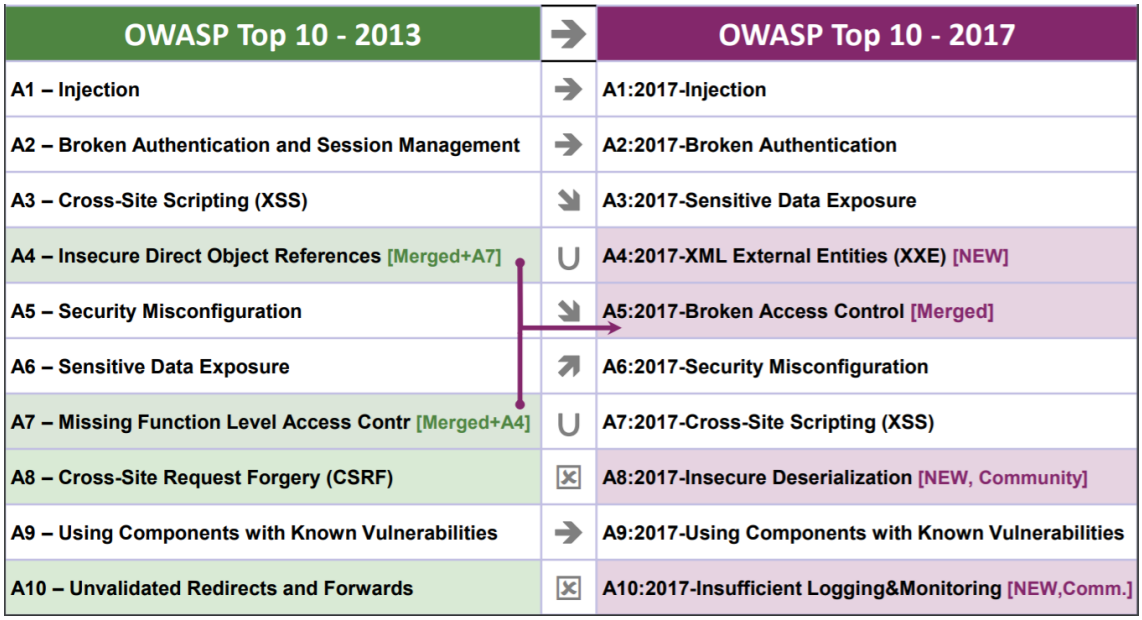


Figura 3-2. **Clasificación de riesgos en aplicaciones web según OWASP Top 10 - 2017**
Fuente: OWASP, 2017

1. **Injection (Inyección)**: Los defectos de inyección de SQL, NoSQL, OS y LDAP, se producen cuando se envían datos no confiables a un intérprete como parte de una consulta. Los datos hostiles del atacante pueden engañar al intérprete para que ejecute comandos no deseados o acceda a los datos sin la autorización adecuada (Fox, 2006).

2. **Broken Authentication (Pérdida de autenticación)**: Las funciones relacionadas con la autenticación y la administración de sesiones de usuario, a menudo se implementan de manera incorrecta, esto da paso a que los atacantes puedan acceder contraseñas, claves o tokens de sesión, o explotar otros defectos de implementación para apropiarse de la información de otros usuarios de manera temporal o permanente (Fox, 2006).

3. **Sensitive Data Exposure (Exposición de datos sensibles)**: Muchas aplicaciones web y API no protegen adecuadamente los datos confidenciales, lo que hace posible que los atacantes pueden acceder o modificar dichos datos débilmente protegidos para realizar fraudes con tarjetas de crédito, robo de identidad u otros delitos. Los datos confidenciales pueden verse comprometidos sin protección adicional, como el cifrado en tránsito, y requieren precauciones especiales cuando se intercambian con el navegador (Fox, 2006).

4. **XML External Entities (XXE):** Muchos procesadores XML antiguos o mal configurados evalúan referencias de entidades externas dentro de documentos XML, se las pueden usar para revelar archivos internos utilizando el controlador de URI de archivo, recursos compartidos de archivos, escaneo de puertos internos, ejecución remota de código y ataques de denegación de servicio (Fox, 2006).

5. **Broken Access Control (Control de acceso incorrecto)**: Los privilegios de los usuarios autenticados no se aplican de manera adecuada, esto ocasiona que los atacantes puedan explotar estas fallas para acceder a datos no autorizados, entre ellas: cuentas de otros usuarios, ver archivos confidenciales, modificar los datos de otros usuarios, cambiar los derechos de acceso, entre otros (Fox, 2006).

6. **Security Misconfiguration (Configuración de seguridad incorrecta)**: Comúnmente es el resultado de permitir o establecer configuraciones predeterminadas, configuraciones incompletas, almacenamiento en la nube abierta, encabezados HTTP mal configurados y mensajes de error detallados que contienen información confidencial. Cada compenente no solo deben estar configurados de manera segura, sino que deben ser actualizados de manera oportuna (Fox, 2006).

7. **Cross-Site Scripting XSS:** Las fallas de XSS ocurren cada vez que una aplicación incluye datos no confiables en una nueva página web sin una validación adecuada, o actualiza una página web existente con datos proporcionados por el usuario utilizando una API de navegador que puede crear HTML o JavaScript. XSS permite a los atacantes ejecutar scripts en el navegador de la víctima que pueden secuestrar sesiones de usuario, desfigurar sitios web o redirigir al usuario a sitios maliciosos (Fox, 2006).

8. **Insecure Deserialization (Deserialización insegura):** Esta falla conduce a la ejecución remota de código. Incluso, pueden usarse para realizar ataques, incluidos ataques de repetición, ataques de inyección y ataques de escalada de privilegios (Fox, 2006).

9. **Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas):** Los componentes, como bibliotecas, marcos y otros módulos de software, se ejecutan con los mismos privilegios que una aplicación web, por lo tanto, si se explota un componente vulnerable, dicho ataque puede facilitar la pérdida de datos o la adquisición del servidor (Fox, 2006).

10. **Insufficient Logging & Monitoring (Registro y monitoreo insuficientes):** El registro y monitoreo insuficientes, junto con la falta de respuesta a incidentes, permite atacar los sistemas, mantener la persistencia, saltar a más sistemas y manipularlos, extraer o destruir datos. La mayoría de los estudios de incumplimiento muestran que el tiempo para detectar un incumplimiento es superior a 200 días, generalmente detectado por partes externas en lugar de procesos internos o monitoreo (Fox, 2006).

2.2.13. Políticas de seguridad

Recoge las directrices u objetivos de una organización con respecto a la seguridad de la información. Forma parte de su política general y, por tanto, ha de ser aprobada por la dirección (Aguilera Lopez, 2010, p. 36).

El objetivo principal de la redacción de una política de seguridad es la de concienciar a todo el personal de una organización, y en particular al involucrado directamente con el sistema de información, en la necesidad de conocer qué principios rigen la seguridad de la entidad y cuáles son las normas para conseguir los objetivos de la seguridad planificados (Aguilera Lopez, 2010, p. 36).

- **Plan de contingencias:** Es un instrumento de gestión que contiene las medidas (tecnológicas, humanas y de organización) que garanticen la continuidad del negocio protegiendo el sistema de información de los peligros que lo amenazan o recuperándolo tras un impacto (Aguilera Lopez, 2010, p. 38).

- **Resiliencia:** es la capacidad de la infraestructura, ya sea de seguridad o de TI, de proveer y mantener un funcionamiento aceptable a pesar de fallas y desafíos a la operación normal, por ejemplo: sobrecargas de trabajo, tráfico malicioso, etc (Woods, 2015, p. 12).

Dicho en otras palabras, son un conjunto de reglas, normas y protocolos de actuación que se encargan proteger la información. Se trata de mitigar los riesgos a los que está expuesta la organización en el mundo digital.

Dussán (2006), en su publicación "Políticas de seguridad informática", menciona los siguientes parámetros que se deben tomar en cuenta al momento de redactar las políticas de seguridad:

- Objetivos y ámbitos
- Realizar un análisis de riesgos informáticos a los que puede estar expuesta la institución y así crear políticas acordes a la realidad de la empresa.
- Trabajar con todos los departamentos que cuenta la empresa ya que ellos son los dueños de los activos y cuentan con la experiencia de las falencias y requerimientos.
- Informar al personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios, riesgos relacionados con los recursos, bienes, y elementos de seguridad.
- Identificar cuáles son los jefes de cada departamento ya que son ellos los que tienen la autoridad de tomar las decisiones de los activos con los que cuenta su departamento.
- Crear las nuevas políticas mediante reuniones con las autoridades de la empresa.
- Designar responsabilidades y penalidades en todos los departamentos con el fin de gestionar la seguridad y asegurar el cumplimiento de las políticas.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, que, ante cambios, las políticas puedan actualizarse oportunamente.

2.2.14. Plan de seguridad

Un plan estratégico de seguridad informática se basa en un conjunto de políticas de seguridad elaboradas que parte desde una evaluación de los riesgos que determinan el nivel de seguridad de una organización. Estas políticas se elaboran a partir de la razón de ser de la entidad, es decir parte desde las características de la empresa, entre ellos la organización, sus activos informáticos y el nivel de tecnología que administra la empresa (Gabriela Hernández Pinto & Alice Naranjo Sánchez, 2006).

La creación de un plan de seguridad permite una vez detectadas las vulnerabilidades en los sistemas informáticos, establecer las medidas necesarias para prevenir y proteger a la organización. Una vez terminado el documento, que no necesariamente debe ser extenso, se debe poner en conocimiento al responsable de la organización para que sea revisado y aprobado. Cuando ha sido aprobado y entendido por la dirección, se procede a sociabilizar al personal de la institución para que conozcan las nuevas medidas que deberán seguir para el mejoramiento institucional (Universidad Internacional de Valencia, 2018).

En el sitio web oficial de la Universidad Internacional de Valencia, se mención los pasos a seguir para la elaboración de un plan de seguridad.

- **Identificación:** Para ello realizar un reconocimiento de todos los activos de la organización, incluyendo al personal, el hardware, software, programas informáticos, servidores, datos que estos manejan y servicios externos (Universidad Internacional de Valencia, 2018).

- **Evaluación de riesgos:** en este se debe reconoce cueles pueden ser los posibles riesgos o ciberataques de igual manera los tipos y alcances que pueden tener los activos anteriormente identificados. Como pueden ser la aparición de virus informáticos, hackers, daños físicos o errores de los empleados (Universidad Internacional de Valencia, 2018).

- **Priorizar la protección:** Una vez reconocidas las amenazas y los daños que estas pueden ocasionar, se puede establecer cuáles son las más importantes e indispensables a proteger. Por ejemplo, se puede determinar que proteger a los servidores es más importante que proteger a los equipos (Universidad Internacional de Valencia, 2018).

- **Tomar las precauciones adecuadas:** Se establecen las nuevas medidas y reglas a tomar para que la organización sea capaz de prevenir riesgos y operar se algo va mal (Universidad Internacional de Valencia, 2018).

CAPÍTULO III

3. DISEÑO DE LA INVESTIGACIÓN

El presente capítulo define el tipo y diseño de investigación, métodos, técnicas e instrumentos con su respectiva validación, con la finalidad de modelar e implementar políticas de seguridad para prevenir vulnerabilidades en la plataforma informática.

3.1. Tipo y diseño de la investigación

En vista que el proceso de este estudio es de naturaleza investigativa y experimental, se definen diferentes métodos y técnicas a través de las cuales se conseguirán tanto las bases teóricas de fundamento, así como las métricas de resultado.

3.1.1. Tipo de la investigación

La presente investigación es de tipo explicativa casual debido a que los datos obtenidos permiten tener resultados puntuales e inmediatos para crear un plan de seguridad basado en la norma ISO 27001, posterior a la experimentación realizada en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo.

3.1.2. Diseño de la investigación

El diseño de la investigación es de tipo experimental, para el cual se utilizó estadística referencial aplicando la prueba Chi-Cuadrado (x^2). Donde se evaluó el nivel de seguridad de la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo, analizando 8 de las 10 vulnerabilidades que se encuentran relacionadas directamente con la arquitectura de dicha plataforma, mismas que se encuentran enmarcadas en el OWASP Top 10-2017.

3.2. Métodos y técnicas de investigación

3.2.1. Método científico

El método científico en este estudio sigue los siguientes pasos:

1. Planteamiento del problema: Se basa en consulta de documentos (Registros, Internet, bibliografía científica, investigaciones realizadas en el país y estadísticas oficiales).

2. Formulación de la hipótesis

3. Levantamiento de la información: Se realizan pruebas de penetración en un ambiente de producción.

4. Análisis e interpretación de resultados: Se analizan los resultados obtenidos para la toma de decisiones, generación de recomendaciones y posibles soluciones.

5. Comprobación de la hipótesis: Se determina si con la implementación del plan de seguridad existirá una mejora significativa en el nivel de seguridad de la plataforma informática de la institución

6. Difusión de resultados: Implementar el plan de seguridad y evaluar el nivel de mejora.

3.2.2. Técnicas de recolección de datos

Las técnicas a utilizar en la presente investigación son las siguientes:

- **Observación:** esta técnica permite obtener información registrada durante el experimento que se obtiene a través de las pruebas de concepto en los escenarios de laboratorio.

- **Experimentación (pruebas):** a través de pruebas de concepto se demuestra que una aplicación o servicio puede ser vulnerable, es decir se realizan experimentos en escenarios de laboratorio.

- **Búsqueda de información:** a través de esta técnica se obtiene fuentes de información avalada por expertos en el tema y validada por la comunidad científica

3.3. Instrumentos de recolección de datos

En la tabla que se presenta a continuación se detallan los instrumentos o herramientas empleados para la recolección de datos:

Tabla 2-3. Instrumentos de recolección de datos

Instrumentos	**Descripción**
Kali Linux	Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.
Otros	**Navegadores web:** Google Chrome, Firefox **Sniffing:** Wireshark, Ettercap, BurpSuite **Escaneo y detección de vulnerabilidades:** Nessus, Zenmap, Vega, BurpSuite **Explotación de vulnerabilidades:** Sqlmal, BurpSuite **Denegación de Servicios:** Synflood **Observación:** Ficha de observación

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

3.4. Fuentes de información

Dentro de las fuentes de obtención de información utilizadas en la presente investigación se mencionan las siguientes:

- **Primaria:**
    - Información obtenida por el investigador en la ejecución de pruebas realizadas en el ambiente de producción.
- **Secundaria:**
    - Artículos publicados en revistas científicas, trabajos de investigación publicados a nivel nacional e internacional con temas afines al investigado.
    - Páginas de internet (páginas oficiales de recursos) que brinden información confiable y especializada.
    - Libros especializados en la biblioteca y electrónicos.

3.5. Planteamiento de la hipótesis

3.5.1. Hipótesis general

La implementación del plan de seguridad propuesto mejorará el nivel de seguridad de la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo.

3.5.2. Identificación de variables

- **Variable independiente:** Plan de seguridad

- **Variable dependiente:** Vulnerabilidades en la plataforma informática

3.5.3. Operacionalización conceptual de variables

Tabla 3-3. Operacionalización de variables

Variable	Tipo	Definición
Plan de seguridad	Independiente	Normas y procedimientos para la prevención de vulnerabilidades en plataformas informáticas
Vulnerabilidades en la plataforma informática	Dependiente	Fallas de seguridad que comprometen la integridad de la plataforma informática

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

3.5.4. Operacionalización metodológica de variables

Tabla 4-3. Operacionalización de variables

Variable	Indicadores	Técnica	Instrumento
Plan de seguridad	Seguridad de la plataforma	Observación	Pruebas
Vulnerabilidades en la plataforma informática	Número de vulnerabilidades escaneadas	Observación	Herramientas de escaneo de vulnerabilidades

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

3.6. Población y muestra

3.6.1. Población

Se considera población al conjunto de todos los elementos a ser evaluados, por lo tanto, para la presente investigación se estableció como población de estudio a la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo. Además, se utilizó el OWASP Top 10-2017 para conocer si la plataforma informática está expuesta ante 8 de los 10 riesgos más críticos de seguridad en aplicaciones web, mismos que se encuentran relacionados directamente con la arquitectura de la plataforma en mención.

3.6.2. Selección de la muestra

En la presente investigación, se estableció como muestra a 8 de las 10 vulnerabilidades descritas en el OWASP Top 10-2017, puesto que, al analizar la arquitectura de la plataforma (lenguaje de programación, base de datos, servidor de aplicaciones, etc), se obtuvo como resultado que solo 8 vulnerabilidades se relacionan directamente con la plataforma y con las herramientas de análisis que se emplearon en esta investigación.

3.7. Metodología para prevenir las vulnerabilidades en plataformas informáticas

La metodología para detectar y prevenir vulnerabilidades que se ha tomado como referencia es la propuesta en el 2014 por Alberto Toledo Díaz, "Tests de penetración. Explotación de vulnerabilidades con Metasploit-framework", la cual habla sobre 4 etapas para realizar una prueba de penetración:

- Fase 1. Recopilación de información (Rastreo y exploración)
- Fase 2. Análisis de vulnerabilidades (Enumeración)
- Fase 3. Explotación (Acceso, escalada de privilegios, daño, borrado de huellas)
- Fase 4. Generación de informes

En este apartado se procede a detallar el resultado obtenido al ejecutar los pasos mencionados en dicha metodología, con la implementación de este procedimiento se revelan las fallas de seguridad que al ser descubiertas por usuarios mal intencionados hubieran ocasionado intermitencia en el servicio ofrecido por la plataforma informática y en el peor escenario llegar a sufrir pérdidas o divulgación de la información privilegiada de los usuarios.

3.7.1. Fase 1. Recopilación de información

En el presente estudio se contó con el respectivo patrocinio y/o autorización de la entidad para realizar las pruebas necesarias (Anexo A), motivo por el cual se pudo realizar un estudio sistemático de los componentes de la plataforma informática del CB-GADM-SD; se emplearon técnicas de ingeniería social que permitieron descubrir la problemática existente, del mismo modo, se procedió a realizar la constatación física de la infraestructura de las instalaciones.

La institución cuanta con un cuartel general cuya construcción se encuentra distribuida en 3 plantas, las mimas que alojan a los siguientes departamentos:

- **Planta baja:** Subjefatura de bomberos, Unidad de Prevención e Ingeniería del Fuego, Archivo, Recaudación e Información
- **Primer piso:** Dirección general, Dirección Jurídica, Dirección de Talento Humano, Dirección de Planificación, Cuarto de servidores
- **Segundo piso:** Dirección Administrativa, Dirección Financiera, Sala de capacitaciones

3.7.1.1 Definición del escenario de trabajo

En la Figura 4, se observa un bosquejo de la estructura de la plataforma informática y la red del presente caso de estudio, del mismo modo, en ella se procede a detallar la información necesaria para proceder a la etapa siguiente; entre la información a listar se tiene el sistema operativo, direcciones IP, enlaces web.

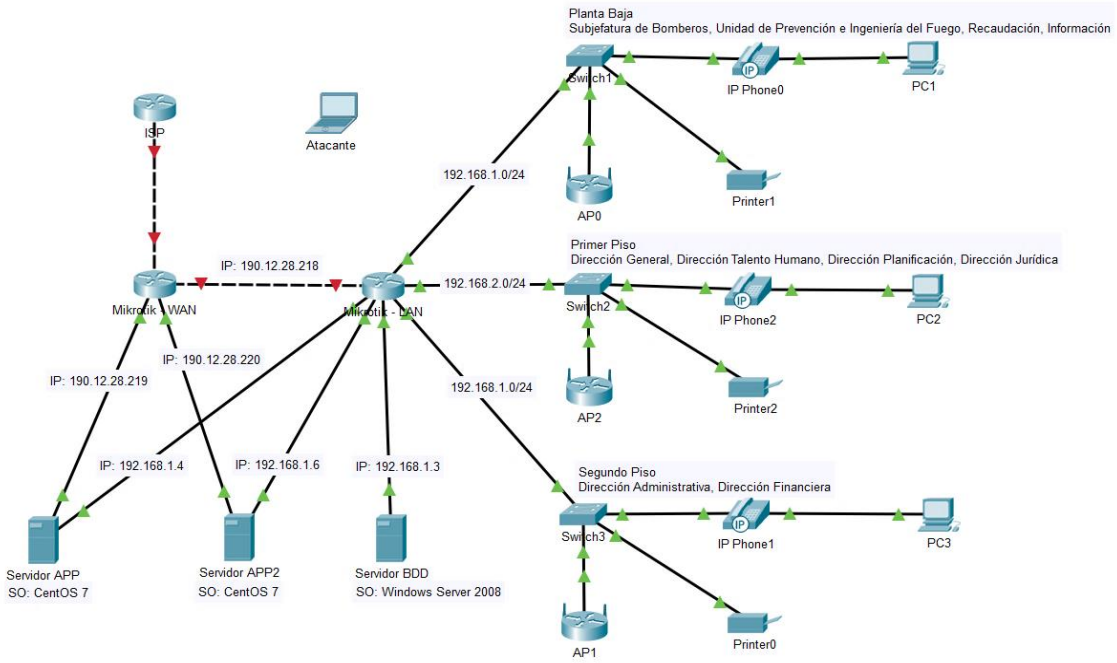


Figura 4-3. **Escenario de trabajo – Infraestructura de la plataforma informática**
Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

3.7.2. Fase 2. Identificación de vulnerabilidades

3.7.2.1 ¿Qué vulnerabilidades se van evaluar?

Para la identificación y escaneo de vulnerabilidades se tomó como guía al listado de riesgos planteado en la actualización de 2017 del Top 10 de OWASP en relación directa con los componentes y/o herramientas de desarrollo de la plataforma informática, por lo tanto, se analizó si la plataforma informática del CB-GADM-SD es vulnerable ante los siguientes ítems:

- A1: Injection (Inyección)
- A2: Broken Authentication (Pérdida de autenticación)
- A3: Sensitive Data Exposure (Exposición de datos sensibles)
- A5: Broken Access Control (Control de acceso incorrecto)

- A6: Security Misconfiguration (Configuración de seguridad incorrecta)
- A7: Cross-Site Scripting XSS
- A9: Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)
- A10: Insufficient Logging & Monitoring (Registro y monitoreo insuficientes)

3.7.2.2 Herramientas para el escaneo de vulnerabilidades

Utilizando el entorno de Kali Linux se ejecutaron las siguientes herramientas para el escaneo y detección de vulnerabilidades:

- Nessus, BurpSuite, Wireshark, Vega, Zenmap (Nmap)

3.7.2.3 Escaneo de vulnerabilidades con Nessus

Se preparó la herramienta Nessus con los filtros para escaneo de vulnerabilidades web, entre los targets a analizar se encuentran los servidores de aplicaciones y bases de datos descritos en la fase de recopilación de información. En la Figura 5 se observa el resultado del escaneo realizado.

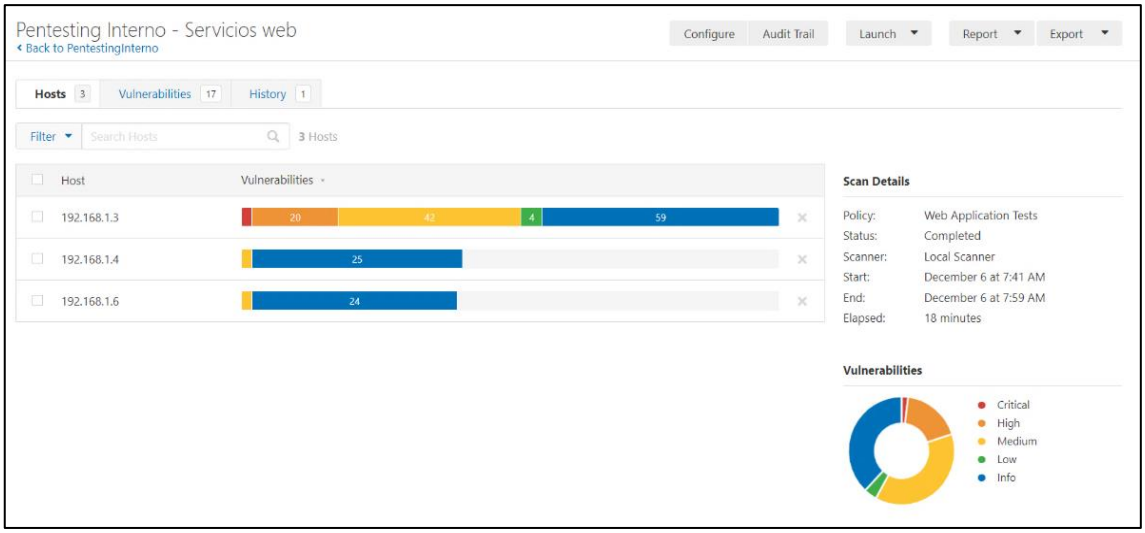


Figura 5-3. **Escaneo de vulnerabilidades a los servidores de aplicaciones y base de datos**
Elaborado por: Pinango Álvaro, 2020

En cuanto a los resultados presentados en la Figura 6, se encuentran relacionados a un filtro aplicado, el cual permite al investigador listar únicamente los resultados que mantengan un "exploit available", es decir, el código CVE para su explotación.

Figura 6-3. **Vulnerabilidades de los servidores de aplicaciones y base de datos relacionados con exploits conocidos**
Elaborado por: Pinango Álvaro, 2020

Según los resultados presentados en las tablas Tabla 5-3 a Tabla 7-3, exportados por Nessus, se relacionan directamente con el ítem A9: Uso de componentes con vulnerabilidades conocidas. Una de las ventajas de usar Nessus, es que brinda al investigador los códigos de explotación de las vulnerabilidades, así como sus posibles soluciones para dar fin a las fallas de seguridad.

Tabla 5-3. Detección de vulnerabilidades en herramienta de desarrollo (PHP)

PHP < 7.1.33 / 7.2.x < 7.2.24 / 7.3.x < 7.3.11 Remote Code Execution Vulnerability			
TARGET: 192.168.1.3			
PUERTO	CVE	SOLUCIÓN	DESCRIPCION
80 / tcp / www	CVE-2019-11043	Upgrade to PHP version 7.3.11 or later.	According to its banner, the version of PHP running on the remote web server is prior to 7.1.33, 7.2.x prior to 7.2.24, or 7.3.x prior to 7.3.11. It is, therefore, affected by a remote code execution vulnerability due to insufficient validation of user input. An unauthenticated, remote attacker can exploit this, by sending a specially crafted request, to cause the execution of arbitrary code by breaking the fastcgi_split_path_info directive.
443 / tcp / www 80 / tcp / www	CVE-2016-1283, CVE-2017-16642	Upgrade to PHP version 5.6.32 or later.	According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.32. It is, therefore, affected by multiple vulnerabilities.
	CVE-2018-7584	Upgrade to PHP version 5.6.34 or later.	According to its banner, the version of PHP running on the remote web server is 5.6.x prior to 5.6.34. It is, therefore, affected by a stack buffer overflow vulnerability.

Nota: Resultados obtenidos relacionados con OWASP Top 10-2017 A9
Elaborado por: Pinango Álvaro, 2020

Tabla 6-3. Detección de vulnerabilidades en herramientas de despliegue de servicios web

Servicios web / Apache HTTP Server (Multiple Issues)			
TARGET: 192.168.1.3			
PUERTO	CVE	SOLUCIÓN	DESCRIPCION
443 / tcp / www 80 / tcp / www	CVE-2019-0196, CVE-2019-0197, CVE-2019-0211, CVE-2019-0215, CVE-2019-0217, CVE-2019-0220	Upgrade to Apache version 2.4.39 or later.	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.39. It is, therefore, affected by multiple vulnerabilities: A privilege escalation vulnerability exists in module scripts due to an ability to execute arbitrary code as the parent process by manipulating the scoreboard. (CVE-2019-0211) An access control bypass vulnerability exists in mod_auth_digest due to a race condition when running in a threaded server. An attacker with valid credentials could authenticate using another username. (CVE-2019-0217) An access control bypass vulnerability exists in mod_ssl when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215) In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-after-free and URL path normalization inconsistencies.
	EDB-ID: 40961 CERT: 797896 BID: 91816, 94650, 95076, 95077, 95078, 105093 CVE: CVE-2016-0736, CVE-2016-2161, CVE-2016-4975, CVE-2016-5387, CVE-2016-8740, CVE-2016-8743	Upgrade to Apache version 2.4.25 or later. Note that the 'httpoxy' vulnerability can be mitigated by applying the workarounds or patches as referenced in the vendor advisory asf-httpoxy-response.txt. Furthermore, to mitigate the other vulnerabilities, ensure that the affected modules (mod_session_crypto, mod_auth_digest,	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.25. It is, therefore, affected by the following vulnerabilities: A flaw exists in the mod_session_crypto module due to encryption for data and cookies using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default). An unauthenticated, remote attacker can exploit this, via a padding oracle attack, to decrypt information without knowledge of the encryption key, resulting in the disclosure of potentially sensitive information. (CVE-2016-0736) A denial of service vulnerability exists in the mod_auth_digest module during client entry allocation. An unauthenticated, remote attacker can exploit this, via specially crafted input, to exhaust shared memory resources, resulting in a server crash. (CVE-2016-2161)

		and mod_http2) are not in use.	The Apache HTTP Server is affected by a man-in-the-middle vulnerability known as 'httpoxy' due to a failure to properly resolve namespace conflicts in accordance with RFC 3875 section 4.1.18. The HTTP_PROXY environment variable is set based on untrusted user data in the 'Proxy' header of HTTP requests. The HTTP_PROXY environment variable is used by some web client libraries to specify a remote proxy server. An unauthenticated, remote attacker can exploit this, via a crafted 'Proxy' header in an HTTP request, to redirect an application's internal HTTP traffic to an arbitrary proxy server where it may be observed or manipulated. (CVE-2016-5387) A denial of service vulnerability exists in the mod_http2 module due to improper handling of the LimitRequestFields directive. An unauthenticated, remote attacker can exploit this, via specially crafted CONTINUATION frames in an HTTP/2 request, to inject unlimited request headers into the server, resulting in the exhaustion of memory resources. (CVE-2016-8740) A flaw exists due to improper handling of whitespace patterns in user-agent headers. An unauthenticated, remote attacker can exploit this, via a specially crafted user-agent header, to cause the program to incorrectly process sequences of requests, resulting in interpreting responses incorrectly, polluting the cache, or disclosing the content from one request to a second downstream user-agent. (CVE-2016-8743)
	BID: 100872 CVE: CVE-2017-9798	Upgrade to Apache version 2.4.28 or later.	According to its banner, the version of Apache running on the remote host is 2.4.x prior to 2.4.28. It is, therefore, affected by an HTTP vulnerability related to the <Limit {method}> directive in an .htaccess file.

Nota: Resultados obtenidos relacionados con OWASP Top 10-2017 A9
Elaborado por: Pinango Álvaro, 2020

Tabla 7-3. Detección de herramienta de desarrollo con vulnerabilidades conocidas

OpenSSL 1.0.x < 1.0.2q Multiple Vulnerabilities			
TARGET: 192.168.1.3			
PUERTO	CVE	SOLUCIÓN	DESCRIPCION
80 / tcp / www	BID: 105758,105897 CVE: CVE-2018-5407, CVE-2018-0734	Upgrade to OpenSSL version 1.0.2q or later.	According to its banner, the version of OpenSSL running on the remote host is 1.0.x prior to 1.0.2q. It is, therefore, affected by a denial of service vulnerability and a cache timing side channel vulnerability.

Nota: Resultados obtenidos relacionados con OWASP Top 10-2017 A9
Elaborado por: Pinango Álvaro, 2020

3.7.2.4 Escaneo de vulnerabilidades con Vega

Con Vega se realizó un escaneo a los dos servidores web mediante su nombre de dominio; en la Figura 7-3 y Figura 8-3 se demuestra que los servidores de aplicaciones son vulnerables ante el ítem A7: Cross-Site Scripting XSS del OWASP Top 10-2017, lo que significa que se encuentran expuestos a que usuarios mal intencionados puedan inyectar código malicioso en la plataforma de servicios en línea para conseguir sus cookies y sesiones de usuarios, modificar el sitio web, realizar HTTP requests con la sesión del usuario, redireccionar a usuarios a sitios dañinos, atacar al navegador o instalar malware, reescribir o manipular extensiones de navegador, entre otras acciones que pueda perjudicar al usuario.

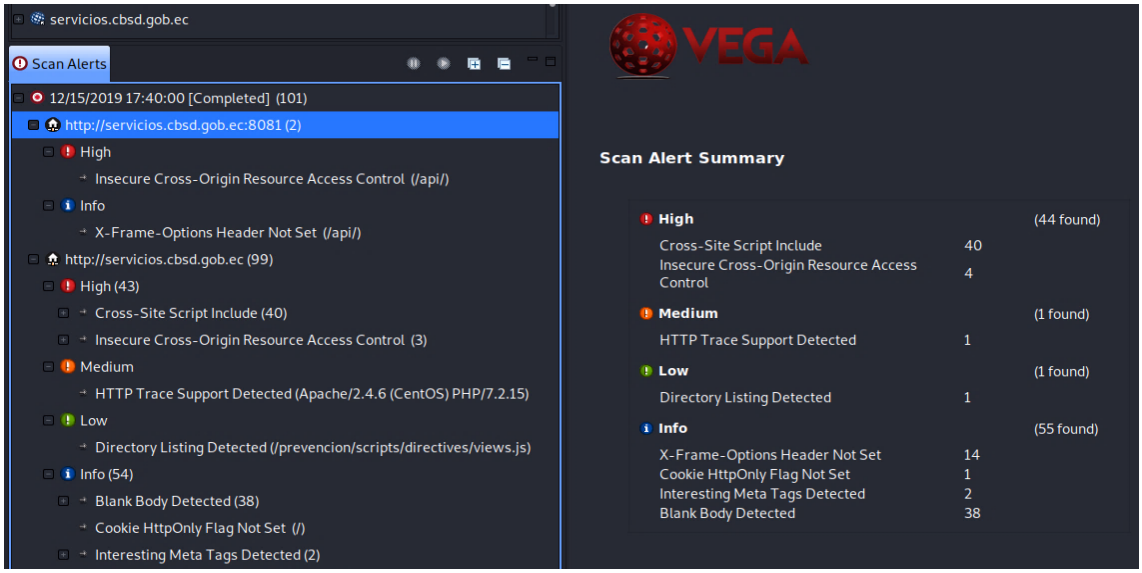


Figura 7-3. **Escaneo de vulnerabilidades al servidor web principal**
Elaborado por: Pinango Álvaro, 2020

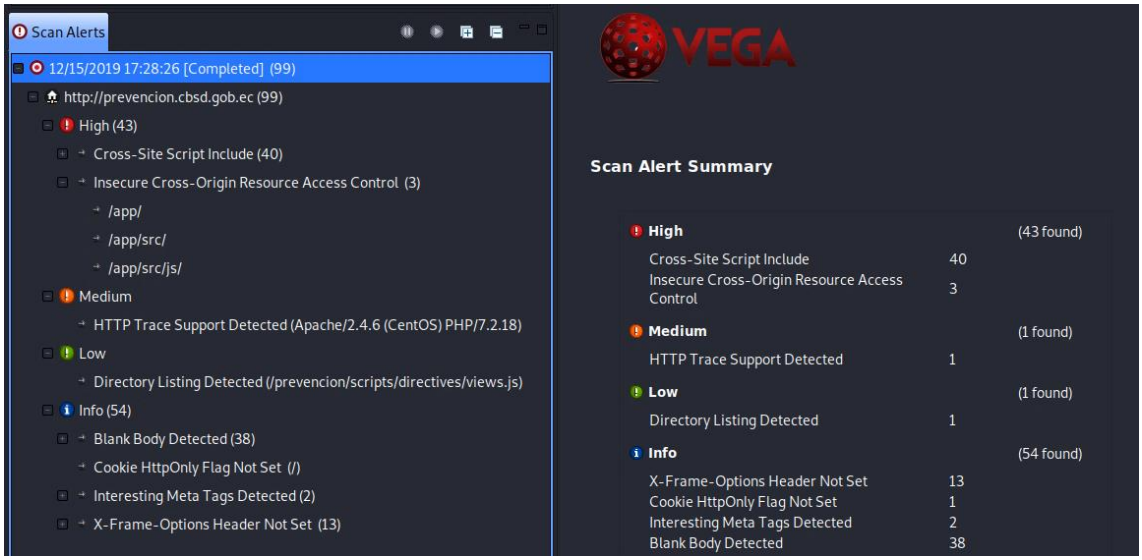


Figura 8-3. **Escaneo de vulnerabilidades al servidor web secundario**
Elaborado por: Pinango Álvaro, 2020

3.7.2.5 Escaneo de vulnerabilidades con Zenmap

En la Figura 9-3 se presenta el resultado del escaneo realizado al equipo de salida a internet (Router MikroTik), la misma que demuestra el estado de los puertos y servicio configurados en el equipo. El escaneo también revela el proveedor del servicio de internet (ISP), configuraciones realizadas al equipo, y métodos HTTP por las cuales se podría llegar a vulnerar al equipo. Según la descripción del OWASP Top 10 el resultado de esta prueba se clasifica dentro del ítem A6: Configuración de seguridad incorrecta.

```
nmap -T4 -A -v 190.12.28.218

Nmap scan report for corp-190-12-28-218.sto.puntonet.ec (190.12.28.218)
Host is up (0.053s latency).
Not shown: 990 closed ports
PORT      STATE    SERVICE        VERSION
22/tcp    open     ssh            MikroTik RouterOS sshd (protocol 2.0)
| ssh-hostkey:
|   1024 96:bf:d7:3c:68:04:ad:20:3e:2c:35:d0:23:08:bf:62 (DSA)
|_  2048 a7:60:77:32:0e:d6:d6:62:df:36:be:1f:7a:1c:cc:13 (RSA)
25/tcp    filtered smtp
53/tcp    open     domain         (generic dns response: NOTIMP)
1723/tcp  open     pptp           MikroTik (Firmware: 1)
2000/tcp  open     bandwidth-test MikroTik bandwidth-test server
5432/tcp  filtered postgresql
8080/tcp  filtered http-proxy
8181/tcp  open     http           nginx
| http-methods:
|_  Supported Methods: GET HEAD
|_http-title: Welcome to nginx!
8291/tcp  open     unknown
49999/tcp open     unknown
```

Figura 9-3. **Escaneo de vulnerabilidades realizado al router MikroTik**
Elaborado por: Pinango Álvaro, 2020

En la Figura 10-3 y Figura 11-3 se presenta el resultado de los escaneos realizados a los servidores de aplicaciones mediante sus nombres de dominio, los resultados más relevantes obtenidos son los siguientes:

- (A3: Exposición de datos sensibles) Ninguno de los servidores de aplicaciones analizados cuenta con el servicio de cifrado de datos presente en el puerto 443 o servicio https, con esto se concluye que las peticiones realizadas entre el navegador y los servidores web se verán expuestas.

- (A5: Control de acceso incorrecto) La configuración por defecto del fichero para navegación ha revelado que existen 3 directorios (app, system, cdn) que no son rastreados por los navegadores, pero que, su navegación por los mismo es posible al desplazarse por un navegador de directorios.

- (A6: Configuración de seguridad incorrecta) El servicio ftp se encuentra con sus configuraciones por defecto o presenta fallas en su configuración, esto lo clasifica directamente en el ítem.

- (A9: Uso de componentes con vulnerabilidades conocidas) El escaneo realizado revela los nombres y las versiones de las herramientas de despliegue de la plataforma, entre ellas se encuentra: Apache httpd 2.4.6, PHP 7.2.15, Node.js Express framework, OpenSSH 7.4

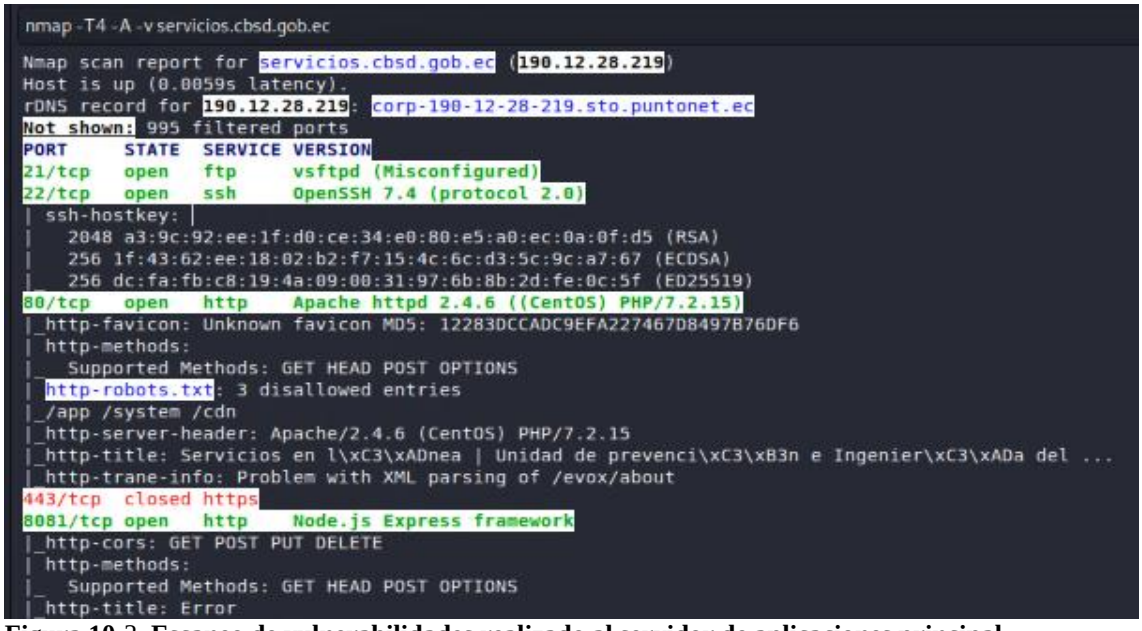


Figura 10-3. **Escaneo de vulnerabilidades realizado al servidor de aplicaciones principal**
Elaborado por: Pinango Álvaro, 2020

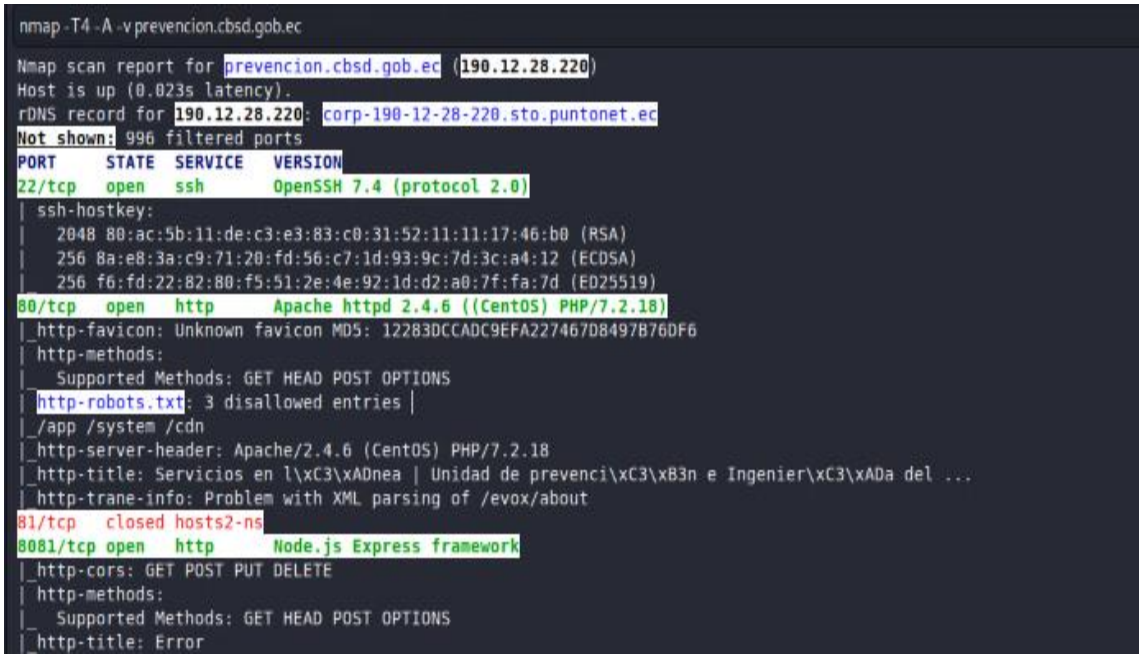


Figura 11-3. **Escaneo de vulnerabilidades realizado al servidor de aplicaciones secundario**
Elaborado por: Pinango Álvaro, 2020

El resultado del escaneo realizado al servidor de base de datos presente en la Figura 12-3, demuestra lo siguiente:

- (A6: Configuración de seguridad incorrecta) El análisis revela la presencia del despliegue de una copia de la aplicación web de la plataforma, sin embargo, en la información entregada por la Unidad de Tecnologías de la institución, este equipo se lo dedicó exclusivamente para base de datos. Por otro lado, el escaneo revela la presencia de puertos abiertos y servicios activos que no están siendo usados, lo que permitirá comprometer de una u otra manera la integridad del equipo.

- (A9: Uso de componentes con vulnerabilidades conocidas) El escaneo realizado revela los nombres y las versiones de las herramientas de despliegue de la plataforma, entre ellas se encuentra: Apache httpd 2.4.23, PHP 5.6.28, OpenSSL 1.0.2j

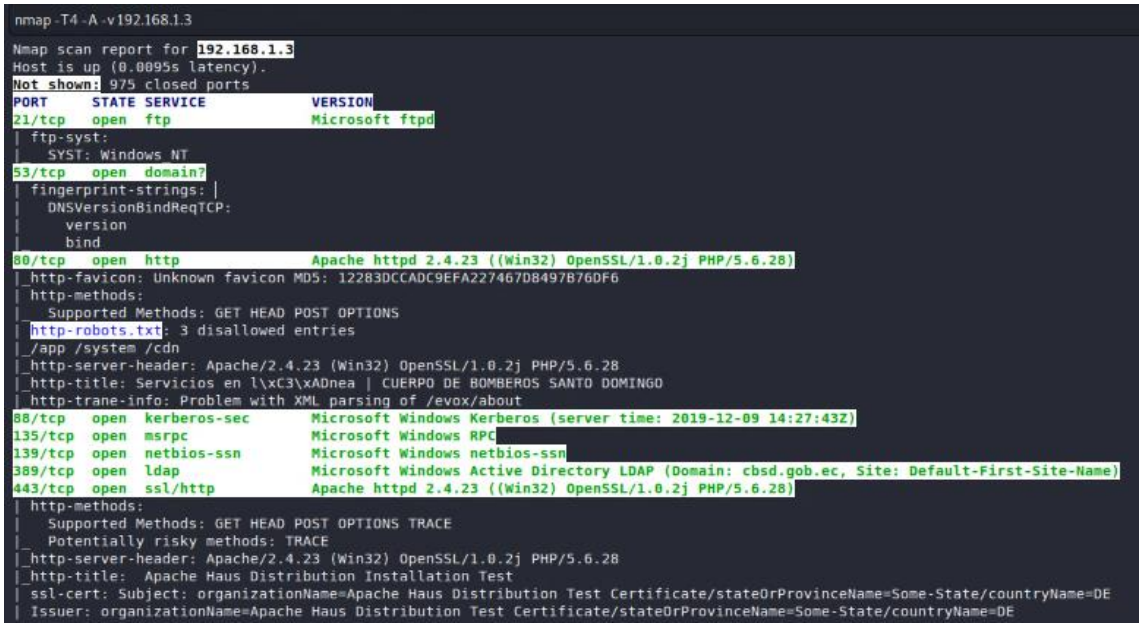


Figura 12-3. **Escaneo de vulnerabilidades realizado al servidor de base de datos**
Elaborado por: Pinango Álvaro, 2020

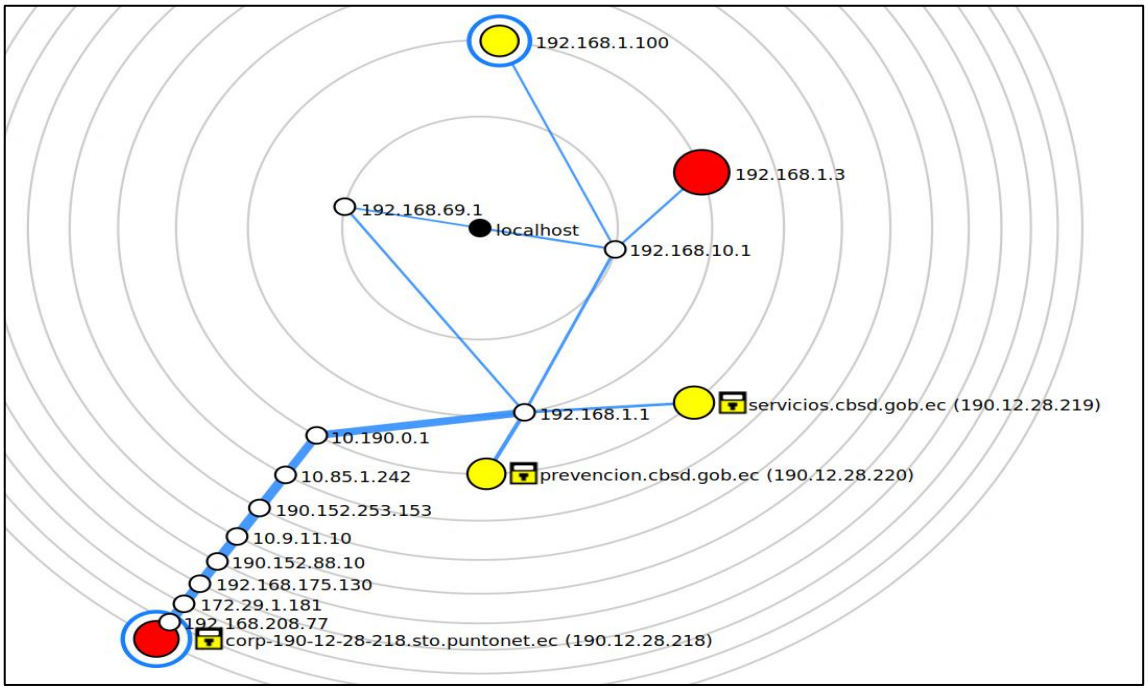


Figura 13-3. **Topología de la red escaneada obtenida por Zenmap**
Elaborado por: Pinango Álvaro, 2020

En la Figura 13-3 se puede apreciar una de las funcionalidades de Zenmap; genera un diseño lógico de las conexiones establecidas para realizar el escaneo, en este se incluyen los saltos, la latencia, nombre de servicio o direcciones IP, etc.

3.7.2.6 Escaneo de vulnerabilidades con Wireshark y BurpSuite

Gracias a la ausencia de implementación del protocolo https en la plataforma, se pudo interceptar los paquetes de navegación, es decir, las peticiones realizadas y respuestas devueltas entre los equipos clientes y el servidor respectivamente, de esta manera se logró obtener la información de la plataforma, entre ellas: credenciales de distintos usuarios mediante los intentos de acceso (inicios de sesión) a la plataforma, información de contactos, entre otras.

En la Figura 14-3 se puede apreciar cómo con tan solo ejecutando la herramienta Wireshark en modo escucha, dentro de la misma red de la víctima, y conociendo la dirección IP de la plataforma informática, se puede capturar los paquetes con la información deseada (A3: Exposición de datos sensibles). Para el caso presentado se ha logrado capturar las credenciales de acceso a la plataforma de un usuario, donde los parámetros enviados son "usuario_login" y "usuario_password", el método http empleado para consultar al servidor es el POST; esta información será de gran utilidad al momento de realizar la explotación de las vulnerabilidades (A2: Pérdida de autenticación).

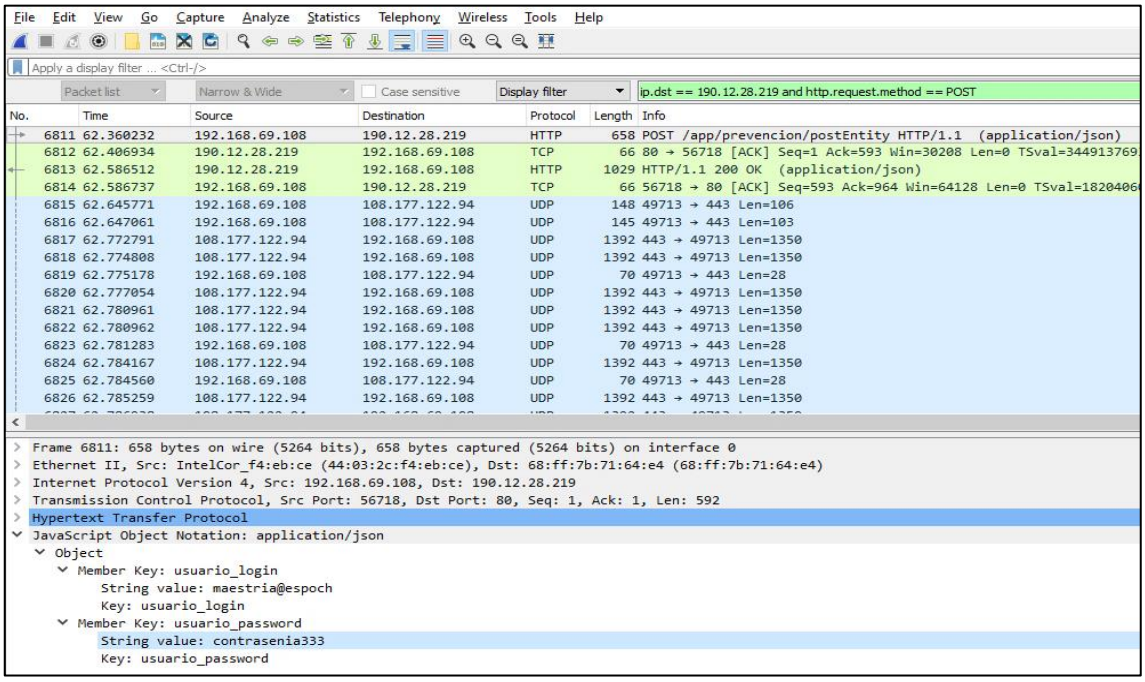


Figura 14-3. **Intercepción de credenciales de acceso para la plataforma de servicios en línea**
Elaborado por: Pinango Álvaro, 2020

En la estación de trabajo del Cuerpo de Bomberos, se configuró en diversos ordenadores de funcionarios la dirección IP de un servidor proxy, para rastrear el tráfico http. En esta etapa se realizó el rastreo de los paquetes relacionados a los datos de sesión de usuario. Con esta práctica se comprobó que la información que se transmite desde el back-end mediante peticiones GET y

POST es devuelta en texto claro sin cifrar, por lo tanto, se exponen datos del usuario ante terceros que se encuentren realizando un filtro de paquetes de la red.

En la Figura 15-3, se comprueba cómo se expone la información de las cuentas bancarias del personal de la institución, puesto que la respuesta devuelta por el servidor no cuenta con ningún tipo de cifrado y los datos son fáciles de entender para cualquier persona (A3: Exposición de datos sensibles).

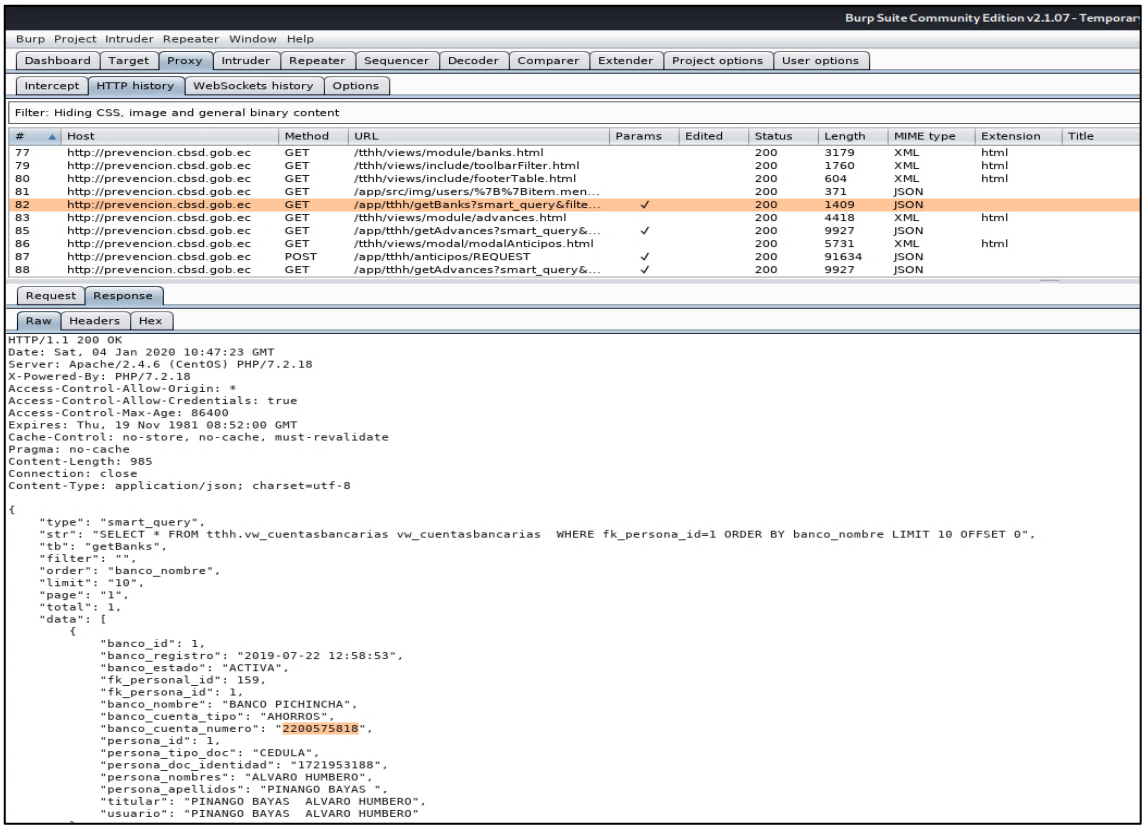


Figura 15-3. **Captura de tráfico de una sesión de usuario en la plataforma informática**
Elaborado por: Pinango Álvaro, 2020

3.7.2.7 Otras técnicas de ingeniería social

En la plataforma se encontró un formulario de registro, el cual permite enviar un dato para consultar si la persona que desea acceder al sitio es o no un usuario registrado. Haciendo uso de este formulario se envió código malicioso para ver la respuesta del back-end; partiendo de los principios básicos de programación donde para comentar código se utilizan los signos/comandos "--, //, **comilla simple**, #, /*, *****/", se envió este tipo de comandos junto con el valor a consultar. Ejemplo: **12345678'--**

En la Figura 16-3, se demuestra cómo el servidor devuelve una consulta errónea, la misma que se debe a un error de sintaxis presente en el lenguaje sql; por lo tanto, el valor enviado desde el

formulario se lo está empleando directamente sin ningún tipo de control en una consulta a la base de datos (A1: Inyección).

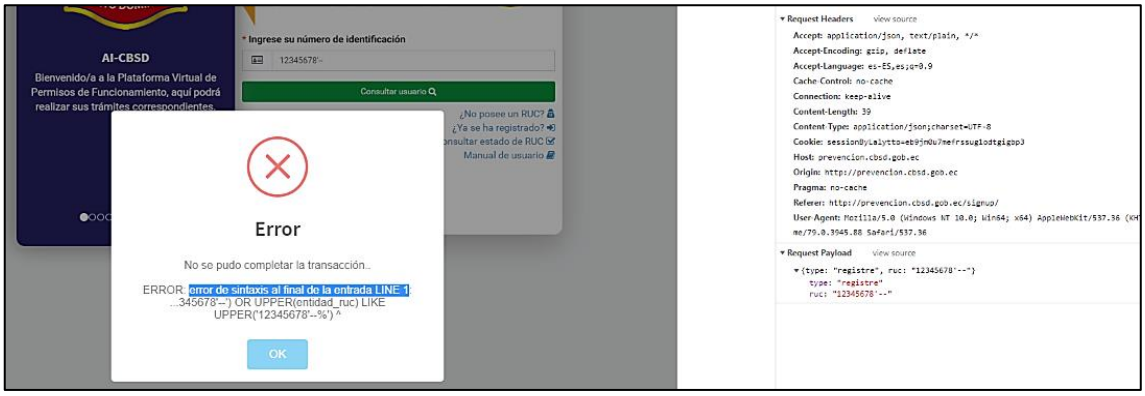


Figura 16-3. **Vulnerabilidad de inyección de código SQL detectada**
Elaborado por: Pinango Álvaro, 2020

Con este ejercicio se obtuvo los datos para una explotación futura (A1: Inyección).

- **URL:** http://prevencion.cbsd.gob.ec/app/prevencion/entidades/REQUEST
- **Método:** POST
- **Datos enviados:** type y ruc

Haciendo uso del formulario de inicio de sesión de servicios en línea se detectó el autocompletado de credenciales de acceso, de aquí se obtuvo un listado IDs de usuario recordados por la aplicación (A6: Configuración de seguridad incorrecta). En la Figura 17 se presenta esta observación.

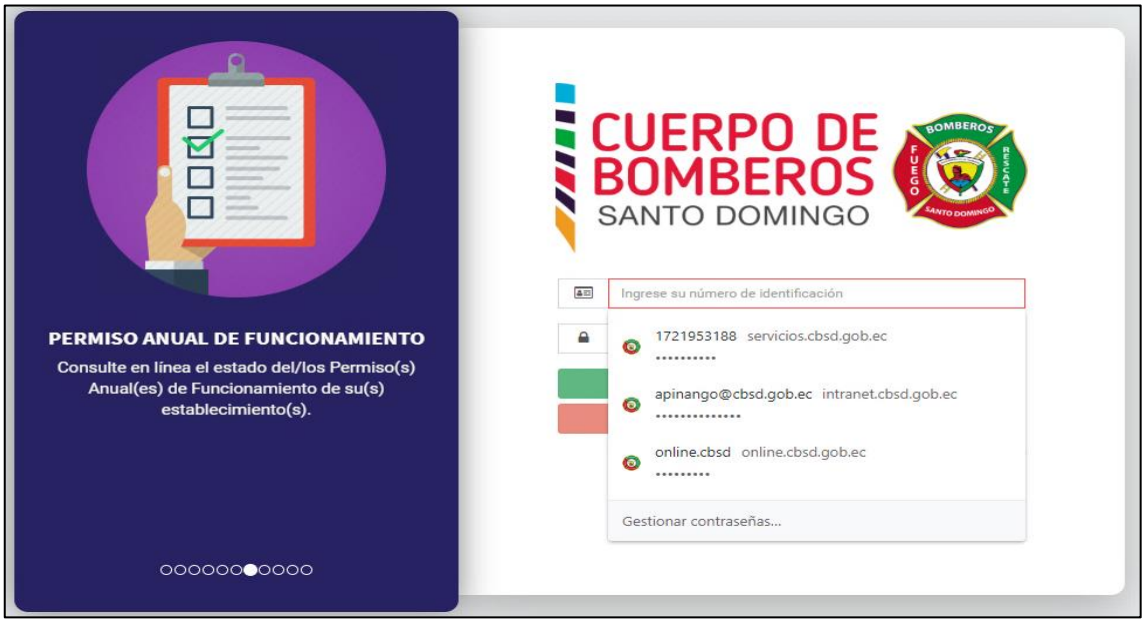


Figura 17-3. **Autorrelleno de credenciales de acceso a la plataforma de servicios en línea**
Elaborado por: Pinango Álvaro, 2020

Adicionalmente, no se presenta ninguna restricción de número de intentos válidos para inicio de sesión, esto significa que, es vulnerable ante los ataques de fuerza bruta o intentos masivos de autenticación (A2: Pérdida de autenticación, A10: Registro y monitoreo insuficientes).

3.7.3. Fase 3. Explotación de vulnerabilidades

En esta fase los equipos fueron sometidos a diversas pruebas de explotación de vulnerabilidades, con el fin de comprobar si se se llegaba a tomar el control de los equipos y/o servicios.

3.7.3.1 Herramientas para explotación de vulnerabilidades

Bajo el mismo entorno de Kali Linux empleado en la fase 2, se ejecutaron las siguientes herramientas para el escaneo y detección de vulnerabilidades:

- Metasploit, BurpSuite, Wireshark, SQLmap

3.7.3.2 A1-Injection (Inyección)

SQLmap permitió explotar la vulnerabilidad de inyección de código SQL, por lo tanto, se consiguió tomar control por completo de la base de datos y de esta manera acceder a información de usuarios, cuentas bancarias, configuraciones del sistema registradas en la base de datos, transacciones realizadas, etc.

En la Figura 18-3 y Figura 19-3 se observa el resultado de la ejecución de la herramienta, la manera cómo descifra la conexión y cómo se comportó el servidor de aplicaciones frente a su ejecución, para esto cabe recalcar que, como resultado permite al investigador (atacante) detalles del motor de base de datos (versión, nombre de base de datos, esquemas, etc).

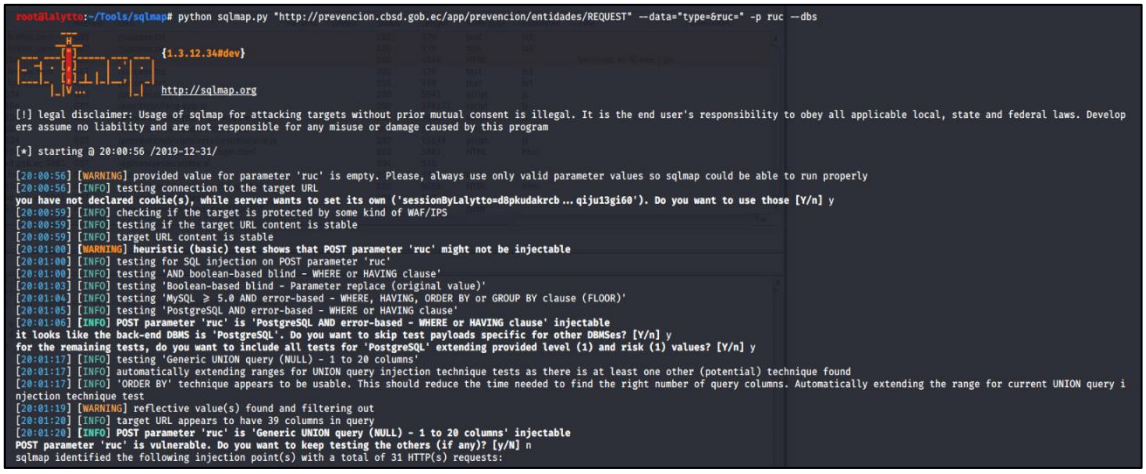


Figura 18-3. **Explotación de vulnerabilidad A1:2017 mediante SQLMap**
Elaborado por: Pinango Álvaro, 2020

Figura 19-3. **Control de la base de datos ejecutando sqlmap**
Elaborado por: Pinango Álvaro, 2020

SQLmap tiene una funcionalidad adicional que permite ejecutar su propia Shell para agilizar la creación y ejecución de consultas sql. En la imagen que se presenta a continuación se puede observar el comando ingresado para ganar la Shell de SQLmap, del mismo modo como se logra obtener información de la tabla de "tb_usuarios" dentro del esquema "admin".

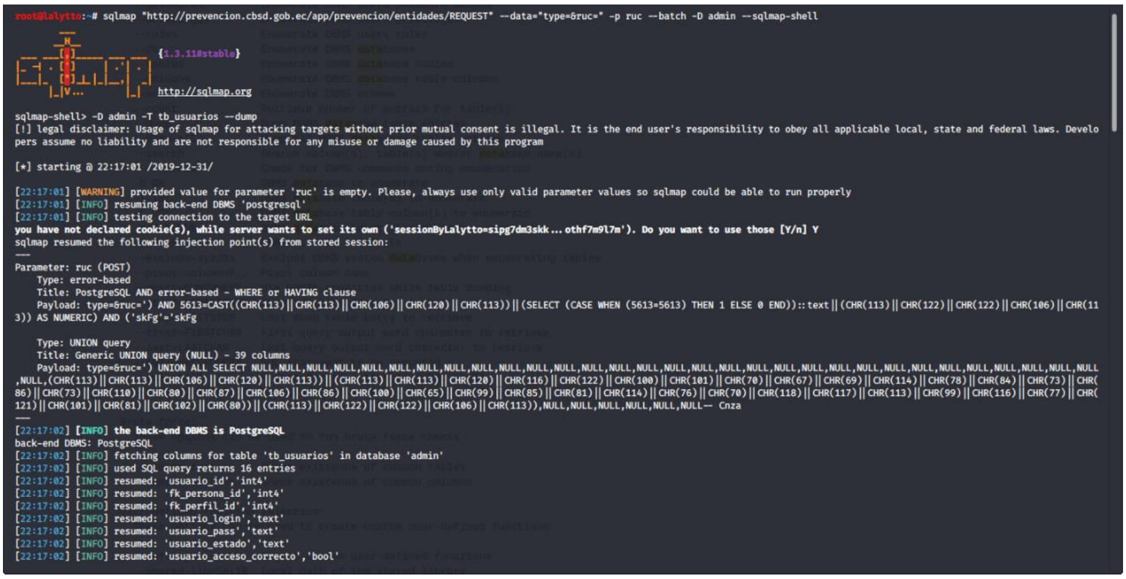


Figura 20-3. **Obteniendo shell sql mediante sqlmap y control de sentencias sql**
Elaborado por: Pinango Álvaro, 2020

3.7.3.3 A2-Broken Authentication (Pérdida de autenticación)

Una vez ganado el acceso a la base de datos se indagó por los esquemas y tablas hasta dar con las tablas en las que se almacena la información de usuarios (credenciales de acceso, nombres, direcciones, teléfonos, etc).

En la Figura 21-3 se puede comprobar que mediante la ejecución de una sentencia que devuelva todas las filas de la tabla de usuarios con SQLmap, al retornar texto cifrado, la misma herramienta proporciona la información del método con el cual ha sido cifrado el texto y trata de descifrarlo. A continuación, se observa el descifrado exitoso de 4 credenciales de acceso dentro de la tabla "**tb_usuarios**" en el esquema "**admin**", con esto se obtiene las credenciales de acceso de usuarios.

Figura 21-3. **Descifrando credenciales de acceso con sqlmap**
Elaborado por: Pinango Álvaro, 2020

Del mismo modo, con la herramienta hydra se puede realizar ataques de fuerza bruta mediante la implementación de diccionarios de contraseñas generadas para realizar estos ataques. Por lo tanto, una vez conocidos los usuarios IDs por falta de seguridad en los formularios de inicio de sesión de la plataforma, en la Figura 22-3 se procede a parametrizar los ataques con la herramienta hydra de la siguiente manera:

hydra -l USUARIO -P /path_wordlist IP_SERVER http-post-form "dirección_login : PARAMETROS_LOGIN : mensaje_error_loggueo".

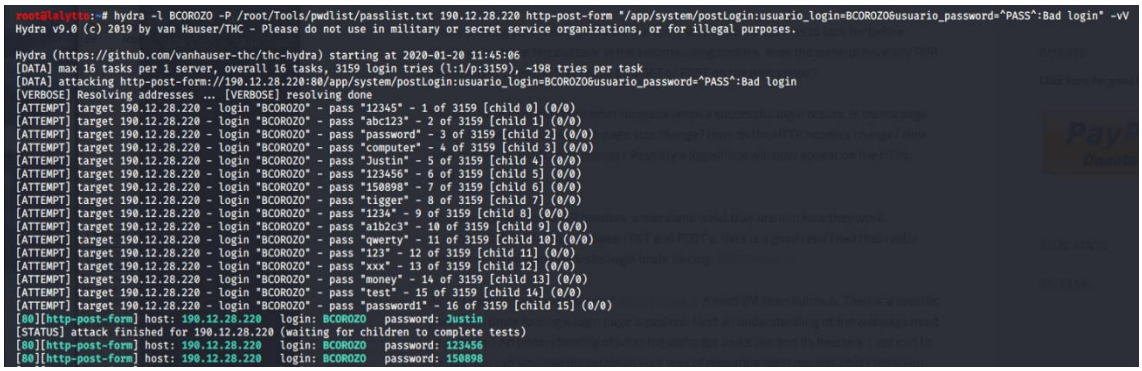


Figura 22-3. **Obtención de contraseñas de usuarios con hydra y diccionarios de datos**
Elaborado por: Pinango Álvaro, 2020

Ettercap, Wireshark y BurpSuite permitieron aprovechar la vulnerabilidad encontrada al momento de realizar un ataque conocido como hombre en el medio, pudiendo interceptar el tráfico de red en el cual se enviaban las credenciales de acceso a la plataforma web.

3.7.3.4 A3-Sensitive Data Exposure (Exposición de datos sensibles)

La técnica que se aplicó para aplicar esta vulnerabilidad fue el filtrado de paquetes de navegación en la plataforma informática, mediante la configuración de servidor proxy realizada a equipos de la red, de los cuales se obtuvieron los paquetes de datos mediante la herramienta BurpSuite.

En la Figura 23-3 se evidencia el rastreo de los paquetes enviados y recibidos entre el equipo cliente y servidor, del listado obtenido se procede a seleccionar una consulta realizada mediante una petición http POST, la misma que da como resultado en la Figura 24 los datos en formato json y en texto sin cifrar.

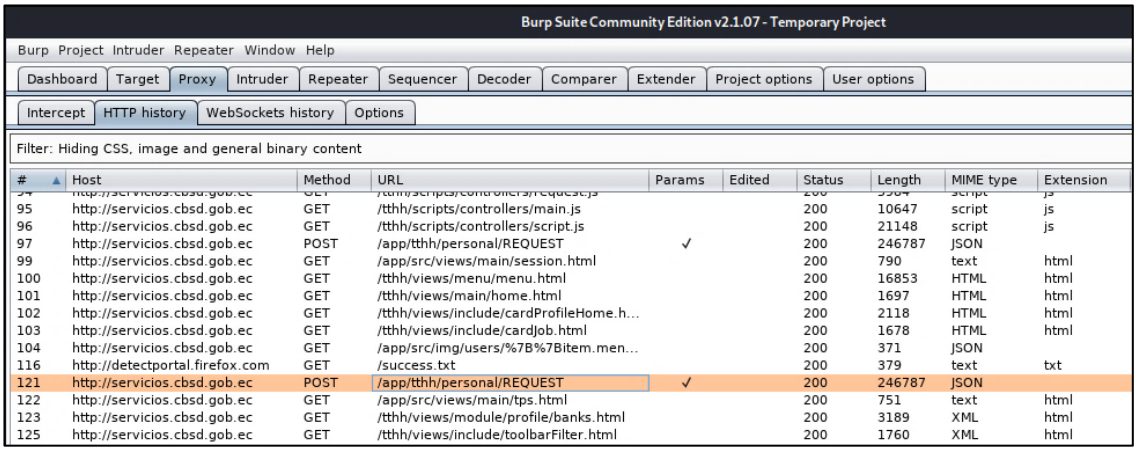


Figura 23-3. **Intercepción de paquetes de navegación en la plataforma informática**
Elaborado por: Pinango Álvaro, 2020

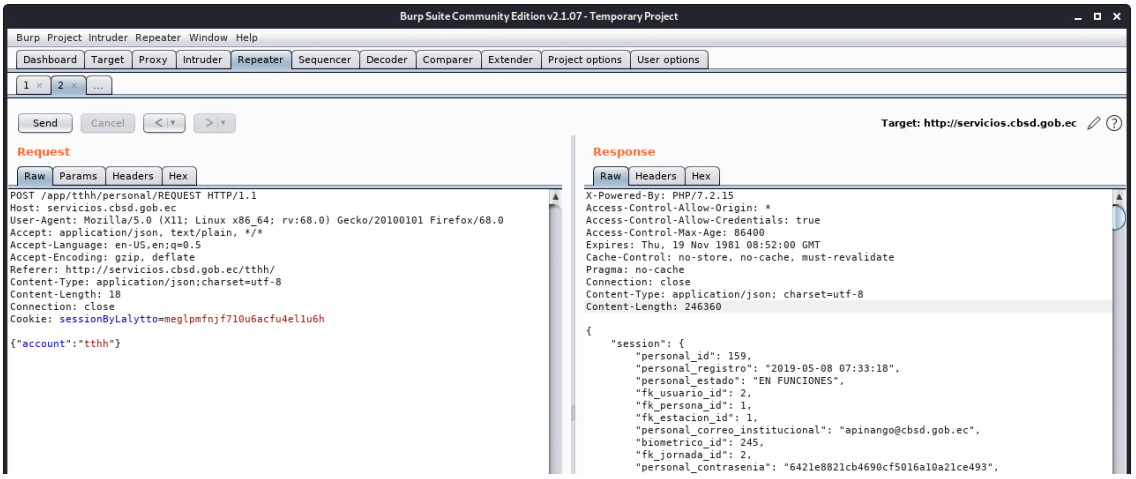


Figura 24-3. **Alteración de sesión de usuario para obtener información sesiones creadas**
Elaborado por: Pinango Álvaro, 2020

Del mismo modo, en las siguientes figuras (Figura 25-3) se presenta el método para visualizar la captura de paquetes filtrados mediante la creación de un hipervínculo para ser visualizado en algún navegador (Figura 26-3), la visualización de los datos capturados se presentan del mismo modo que se presentó en la Figura 24-3, en texto plano sin cifrar.

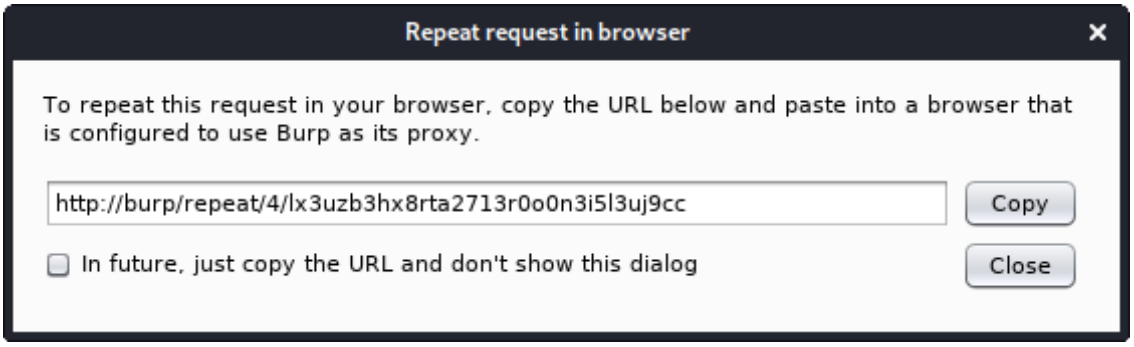


Figura 25-3. **Creación de link para enviar la petición POST al backend desde el navegador**
Elaborado por: Pinango Álvaro, 2020

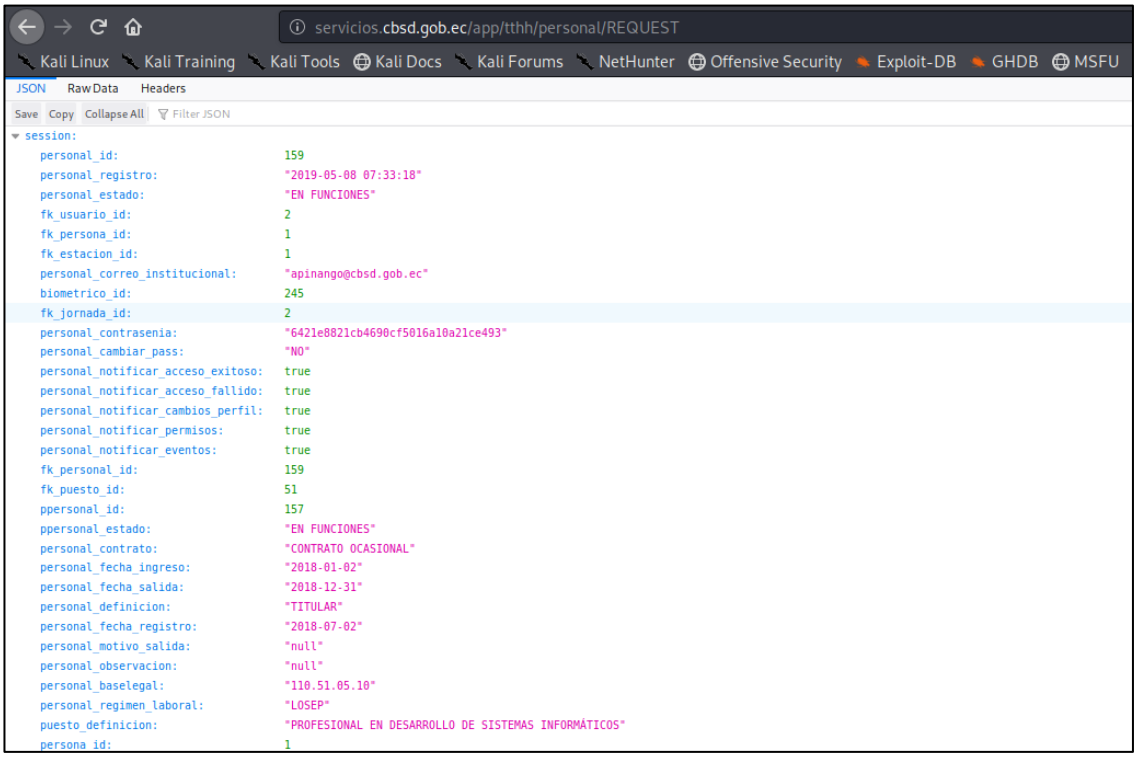


Figura 26-3. **Regreso de información de sesión creada sin cifrar desde backend**
Elaborado por: Pinango Álvaro, 2020

La exposición de datos es evidente al obtener acceso a la misma, aun sabiendo que la solicitud que se estaba realizando era una petición POST.

3.7.3.5 A5-Broken Access Control (Pérdida de control de acceso)

La mayoría de plataformas informáticas generan las consultas y navegación por sus sitios cuando el sitio cambia o actualiza los hipervínculos (URLs de navegación), lo que hace posible cambiar privilegios al cambia manualmente la URL si se conoce lo suficiente las direcciones. Para este caso dentro del aparatado del módulo de Talento Humano se realizó la modificación de la URL para acceder a sitios que usualmente están habilitados únicamente para usuarios administradores

o de más alto privilegio que el usuario que ha iniciado sesión. En la siguiente figura se muestra cómo cambiando la url de navegación no restringe el acceso a dicha ruta de acceso.

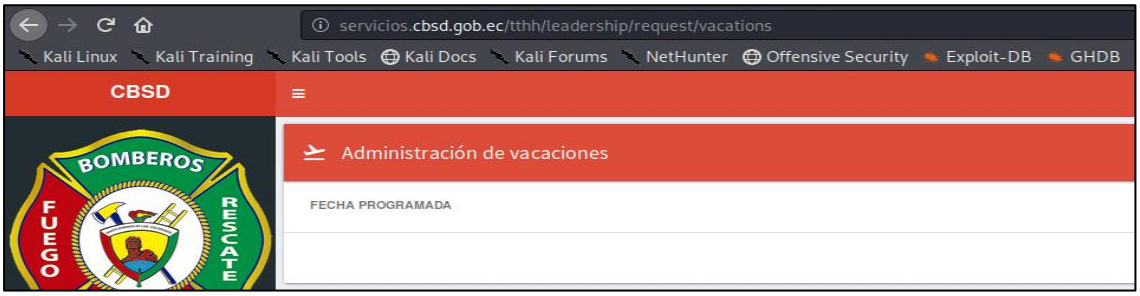
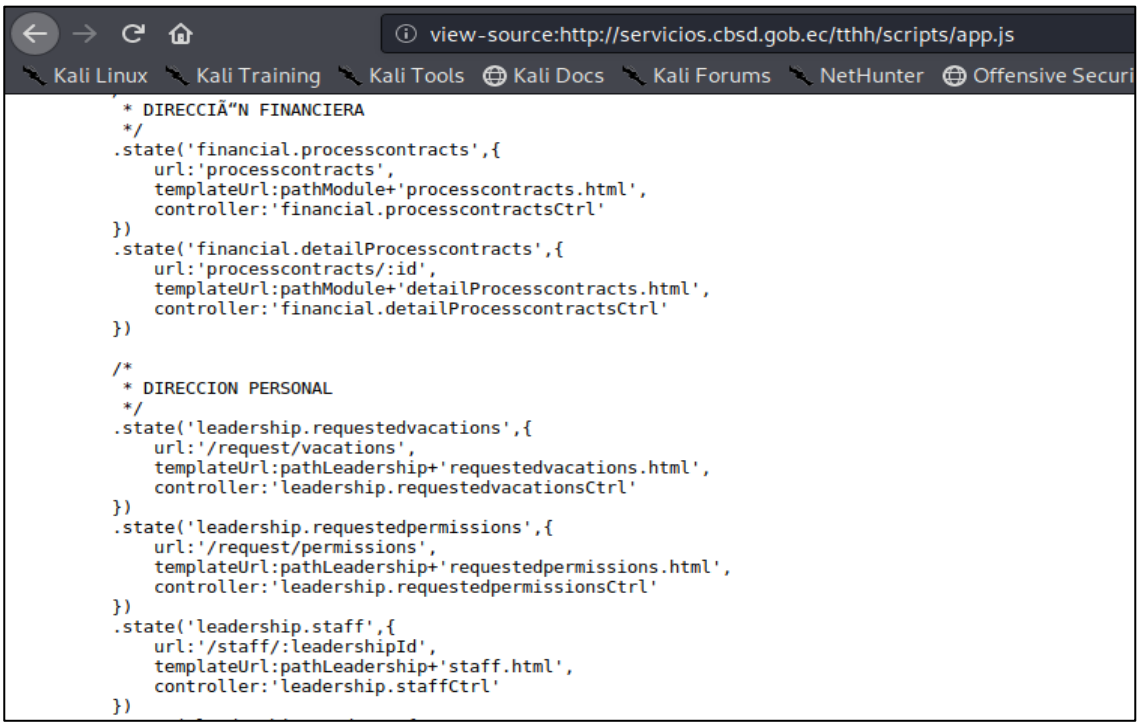


Figura 27-3. **Navegación por el sitio web alterando manualmente la URL de acceso**
Elaborado por: Pinango Álvaro, 2020

Con el fin de emitir un aval para lo demostrado en la Figura 27-3, se procede a detallar en la siguiente figura (Figura 28-3) el contenido del fichero que contiene la configuración de las rutas de navegación por la plataforma.




```
 * DIRECCIÃ"N FINANCIERA
 */
.state('financial.processcontracts',{
    url:'processcontracts',
    templateUrl:pathModule+'processcontracts.html',
    controller:'financial.processcontractsCtrl'
})
.state('financial.detailProcesscontracts',{
    url:'processcontracts/:id',
    templateUrl:pathModule+'detailProcesscontracts.html',
    controller:'financial.detailProcesscontractsCtrl'
})

/*
 * DIRECCION PERSONAL
 */
.state('leadership.requestedvacations',{
    url:'/request/vacations',
    templateUrl:pathLeadership+'requestedvacations.html',
    controller:'leadership.requestedvacationsCtrl'
})
.state('leadership.requestedpermissions',{
    url:'/request/permissions',
    templateUrl:pathLeadership+'requestedpermissions.html',
    controller:'leadership.requestedpermissionsCtrl'
})
.state('leadership.staff',{
    url:'/staff/:leadershipId',
    templateUrl:pathLeadership+'staff.html',
    controller:'leadership.staffCtrl'
})
```

Figura 28-3. **Archivo JavaScript de configuración de rutas privadas del sitio web**
Elaborado por: Pinango Álvaro, 2020

Del mismo modo, se ha detectado que al cargar una nueva ruta se realiza una petición al backend para donde se completarán los datos de la interfaz de usuario. En la figura a continuación se observa la respuesta del servidor ante la consulta realizada que no cuenta con permisos de usuario.

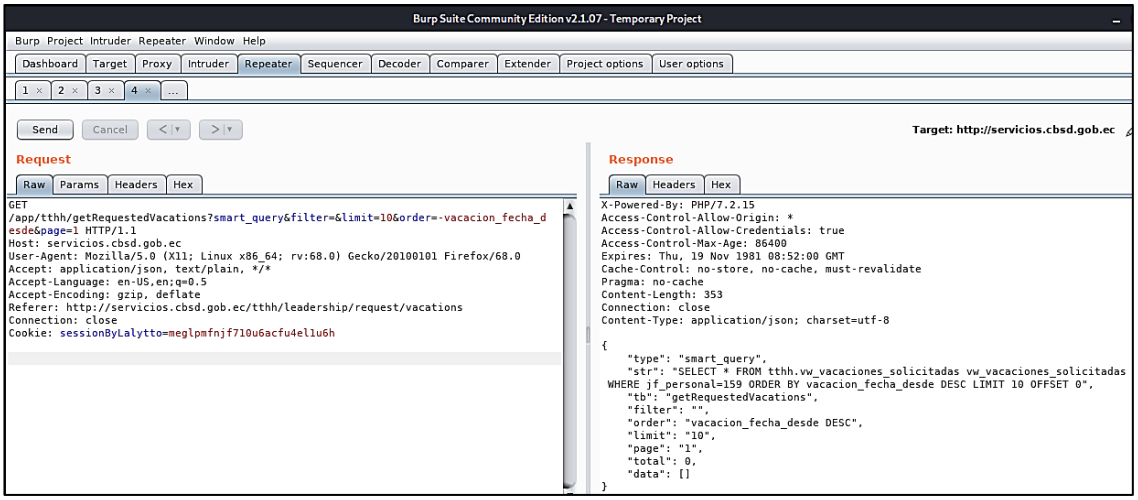


Figura 29-3. **Petición realizada al back-end desde una URL privilegiada**
Elaborado por: Pinango Álvaro, 2020

Como se pudo observar en las imágenes anteriores, BurpSuite permitió explotar la vulnerabilidad de la plataforma informática al cambiar las direcciones url manualmente para navegar por el sitio, de esta manera se obtuvo las peticiones realizadas al back-end para el llenado de datos del usuario; del mismo modo permite modificar las peticiones realizadas las veces que sean necesarios y volverlas a enviar una y otra vez después de nuestras modificaciones.

3.7.3.6 A6 -Security Misconfiguration (Control de seguridad incorrecta)

La configuración por defecto o configuración débil fue la razón por la cual se pudo realizar con éxito la prueba de DoS (Denegación del Servicio); este ataque se realizó mediante las herramientas de Metasploit, synflood.

En la siguiente figura se puede apreciar el ataque realizado al servidor de aplicaciones mediante un ataque conocido como inundación de paquetes (synflood), este ataque se logró por no configurar apropiadamente el número máximo de peticiones simultaneas por IP.

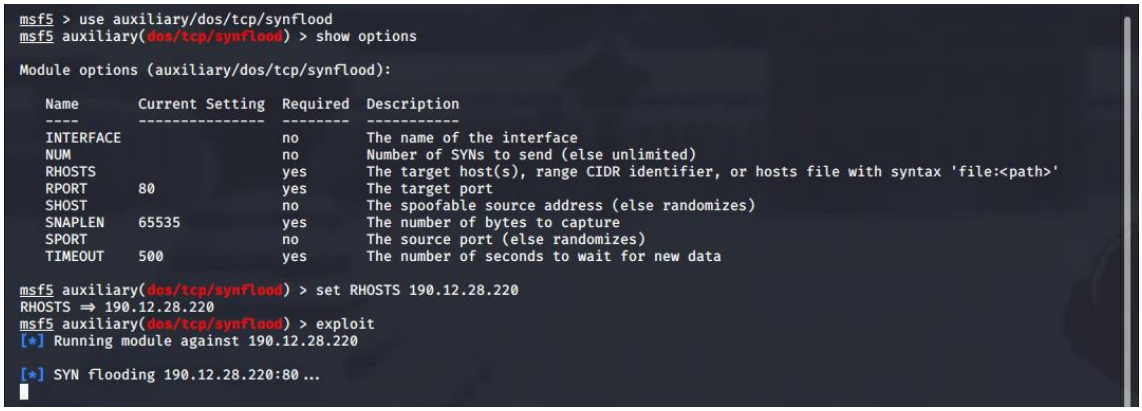


Figura 30-3. **Ejecución de Synflood para denegación de servicio a los servidores de aplicaciones**
Elaborado por: Pinango Álvaro, 2020

Del mismo modo en la Figura 31-3 se presenta el resultado de este ataque, el cual es la denegación o caída total del servicio de la plataforma informática.

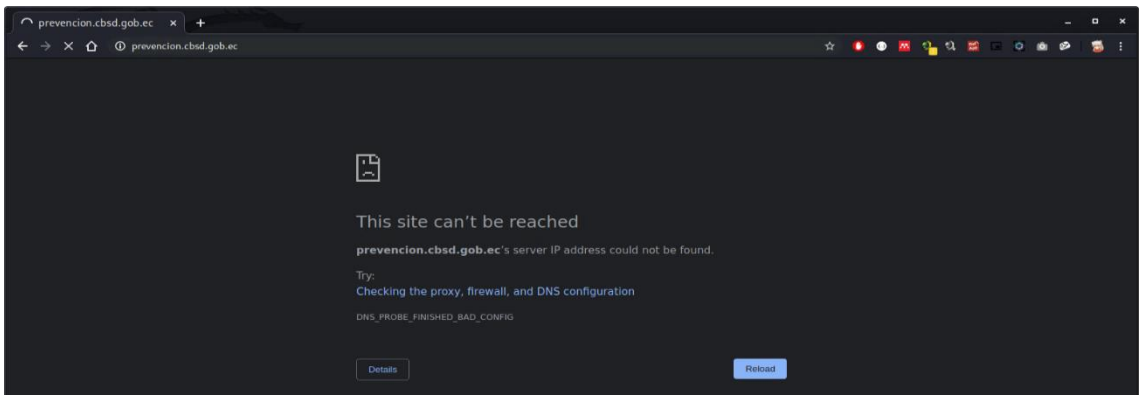


Figura 31-3. **Resultado de la ejecución de synflood en metasploit - caída del servicio**
Elaborado por: Pinango Álvaro, 2020

Al igual que en el ejemplo anterior, mediante la navegación por los directorios realizado BurpSuite (Figura 32-3), se determinó que existen directorios que no se ha restringido el acceso a su contenido, por lo tanto, fácilmente se podría listar todos los recursos necesarios para el funcionamiento de la plataforma y ser utilizado en otros ambientes.

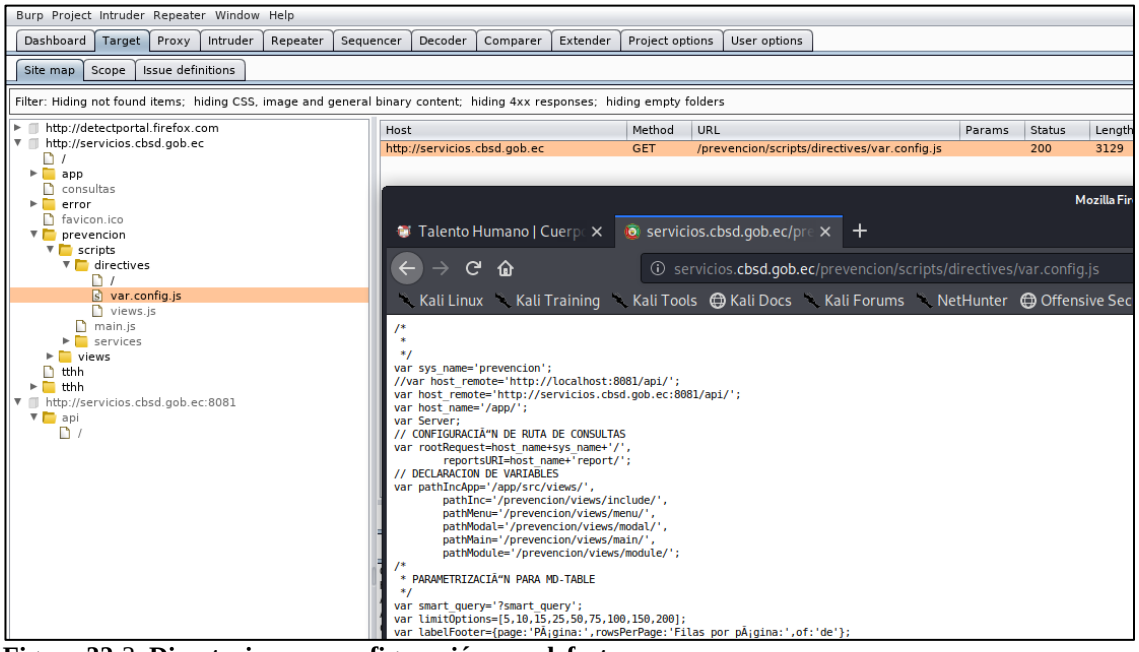


Figura 32-3. **Directorios con configuración por defecto**
Elaborado por: Pinango Álvaro, 2020

3.7.3.7 A7-Cross-Site Scripting (XSS)

Al introducir código malicioso (javascript) en la plataforma informática mediante el envío de datos desde un formulario en la interfaz gráfica de usuario se consiguió explotar esta vulnerabilidad y así conseguir información del usuario. A continuación, se detalla el procedimiento realizado con la herramienta Beef de Kali Linux.

En la Figura 33-3 se inicia Beef, con esta herramienta se va a simular un servidor espía (socket) esperando que el quipo víctima establezca la conexión mediante la carga de un fichero en su despliegue, este fichero es proporcionado en la configuración de Beef, para el presente caso se obtiene las siguientes herramientas:

- Fichero javascript: http://192.168.69.108:3000/hooj.es
- Interfaz de usuario de Beef: http://192.168.69.108:3000/ui/panel

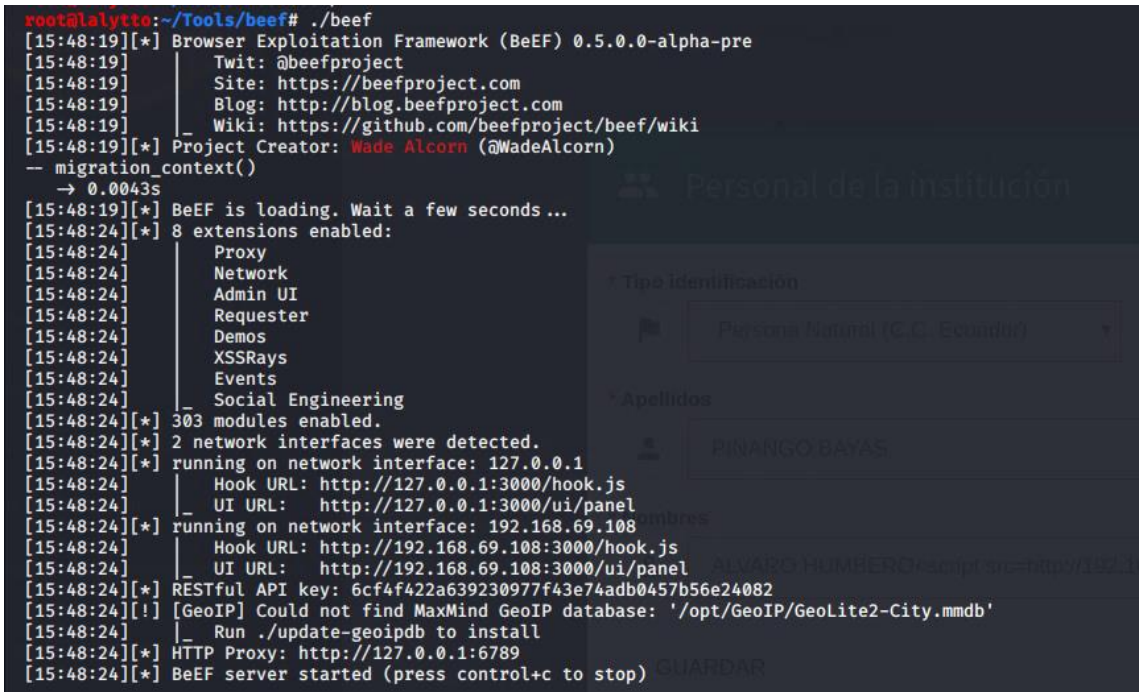


Figura 33-3. **Inicialización de los parámetros de la herramienta Beef**
Elaborado por: Pinango Álvaro, 2020

Una vez iniciado el servicio de Beef se procede a la inyección del fichero javascript que establece la conexión. Se buscó un formulario que permita visualizar en la interfaz de usuario los datos enviados al servidor. El proceso realizado en la siguiente figura permitió el envío y guardado del enlace al fichero javascript para la conexión con Beef.

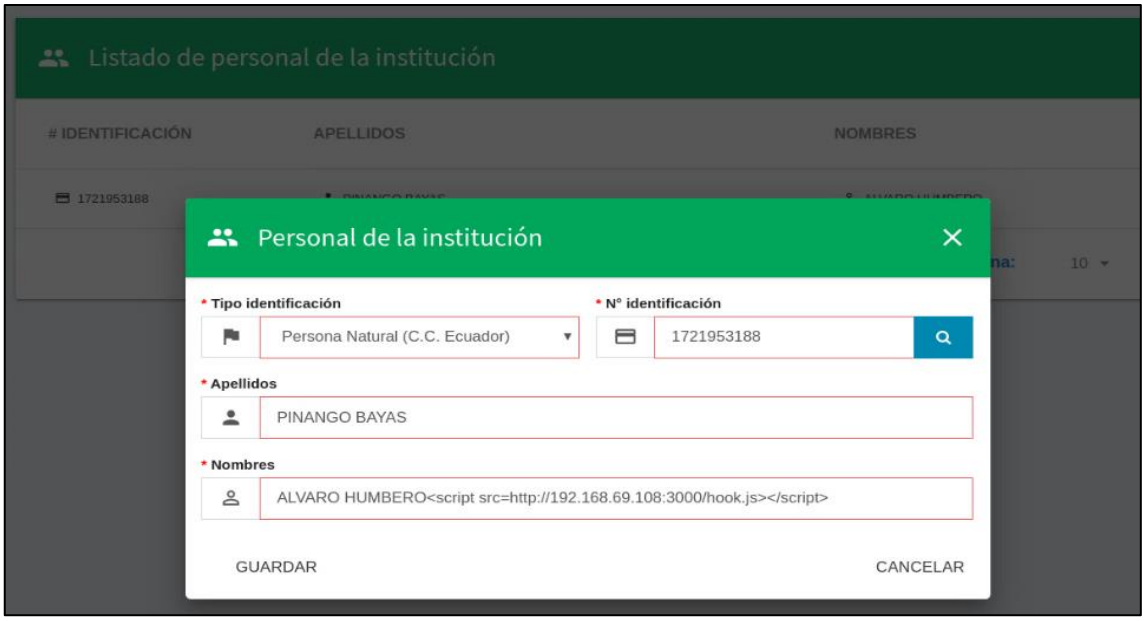


Figura 34-3. **Inyección de código JavaScript para la activación de socket y explotación de vulnerabilidad**
Elaborado por: Pinango Álvaro, 2020

Para comprobar que se está ejecutando el código ingresado se hace uso del inspector de elementos de Google Chrome para visualizar las etiquetas HTML y comprobar la conexión establecida (Figura 35-3).

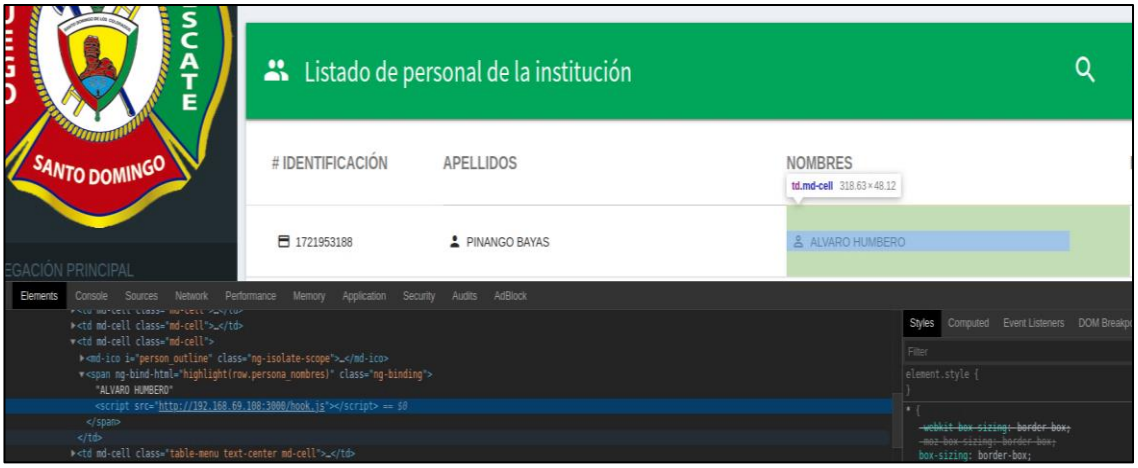


Figura 35-3. **Inspección del código inyectado en la aplicación**
Elaborado por: Pinango Álvaro, 2020

En la Figura 36-3 se observa los navegadores que han sido interceptados mediante la ejecución del javascript en el lado del cliente (navegadores), cabe recalcar que la ejecución de este fichero es independiente del navegador en el que haya sido ingresado, sin embargo, sí depende de la red en la que se esté ejecutando Beef.

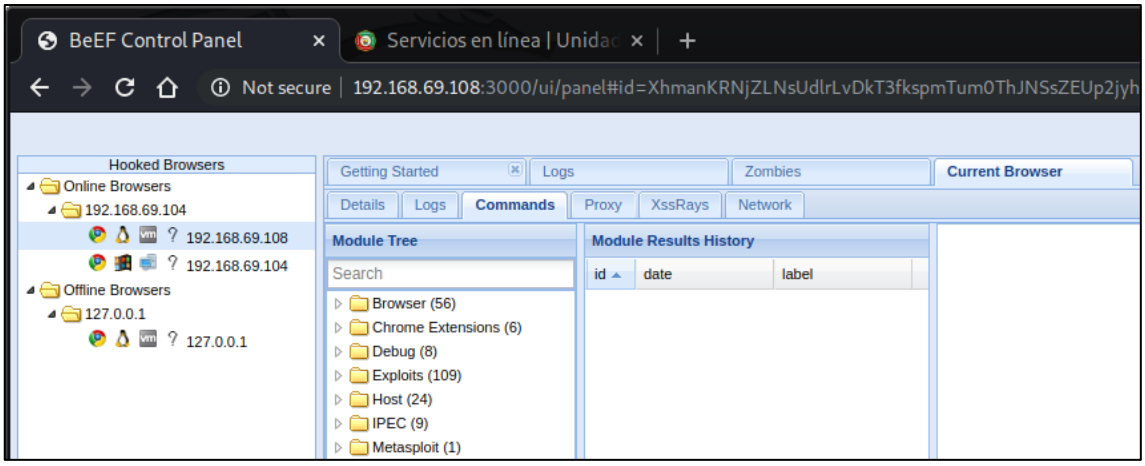


Figura 36-3. **Lista de hosts que han ejecutado la aplicación con código inyectado (XSS)**
Elaborado por: Pinango Álvaro, 2020

En las Figura 37-3 se logró capturar las cookies de sesión del navegador, asimismo en la Figura 38-3 se capturó las configuraciones establecidas con Java. Existen un sinnúmero de opciones que permite al investigar conseguir información privilegiada de los equipos de la víctima.

Figura 37-3. **Lista de ataques y obtención de Cookies del navegador de la víctima**
Elaborado por: Pinango Álvaro, 2020

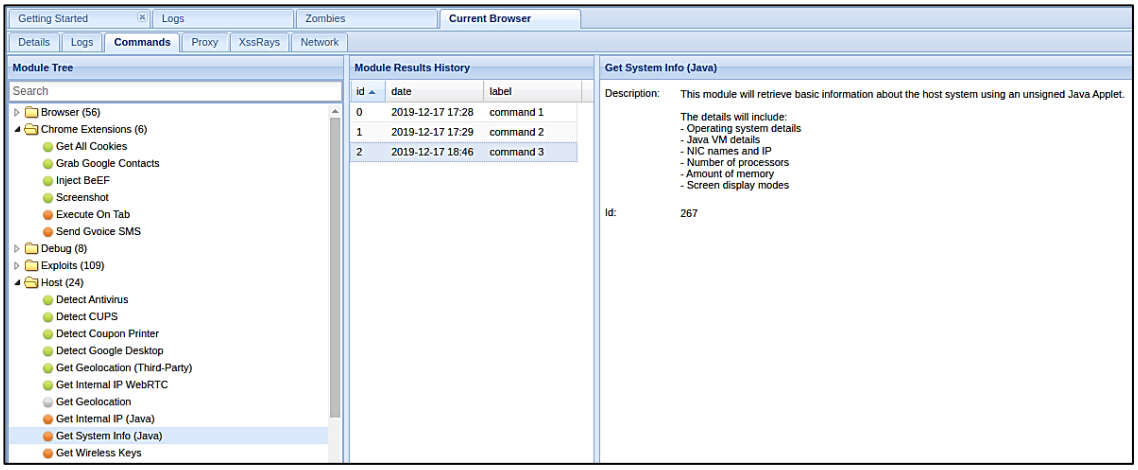


Figura 38-3. **Información de componentes del host vulnerado**
Elaborado por: Pinango Álvaro, 2020

3.7.3.8 A9-Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)

La plataforma informática estudiada hace uso de Apache http (servidor web) para el despliegue de la aplicación; en etapa de escaneo de vulnerabilidades (fase 2) se logró obtener los CVEs para la explotación de las vulnerabilidades de esta herramienta. En este procedimiento, mediante la herramienta Metasploit de Kali Linux se vulneró la seguridad de Apache.

En las siguientes imágenes presentadas a continuación, se puede detallar el resultado de la explotación desde una terminal ejecutando metasploit. Empezando en la Figura 39-3 donde se confirma la información del servidor con la herramienta nmap, se procedió a ejecutar metasploit.

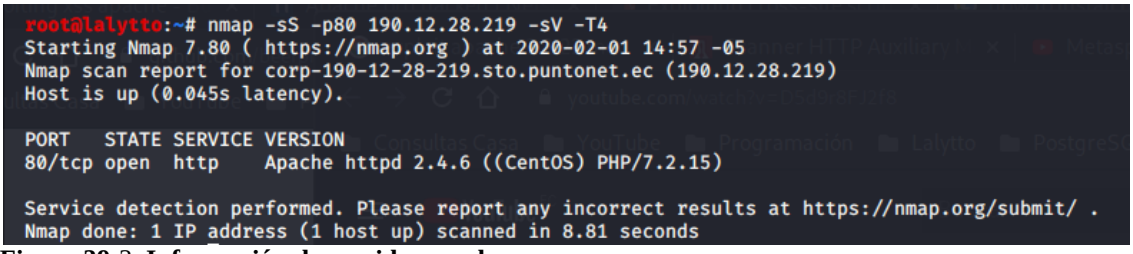


Figura 39-3. **Información de servidor a vulnerar**
Elaborado por: Pinango Álvaro, 2020

Haciendo uso de metasploit se inició con la ejecución del exploit twiki y se procedió a la revisión de los parámetros necesarios para lanzar el ataque. En la Figura 40 se aprecia la inicialización del servicio, mientras que, en la Figura 41 se establecen los datos del servidor víctima y se procede a lanzar el ataque.

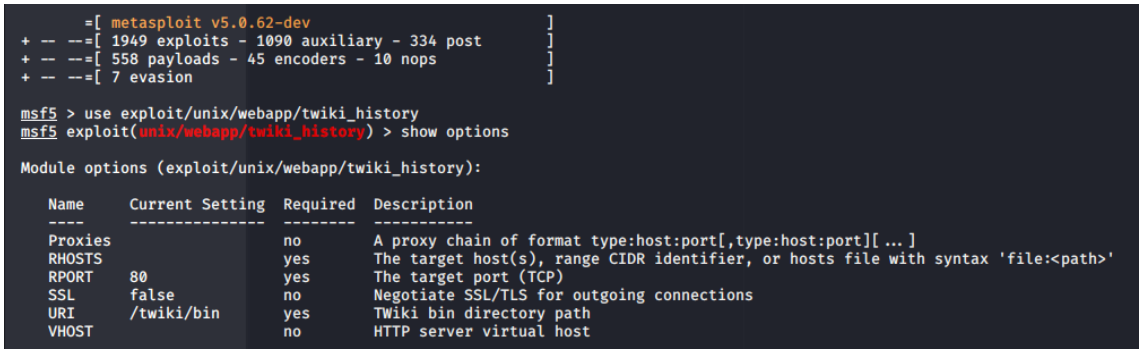


Figura 40-3. **Inicialización de exploit**
Elaborado por: Pinango Álvaro, 2020

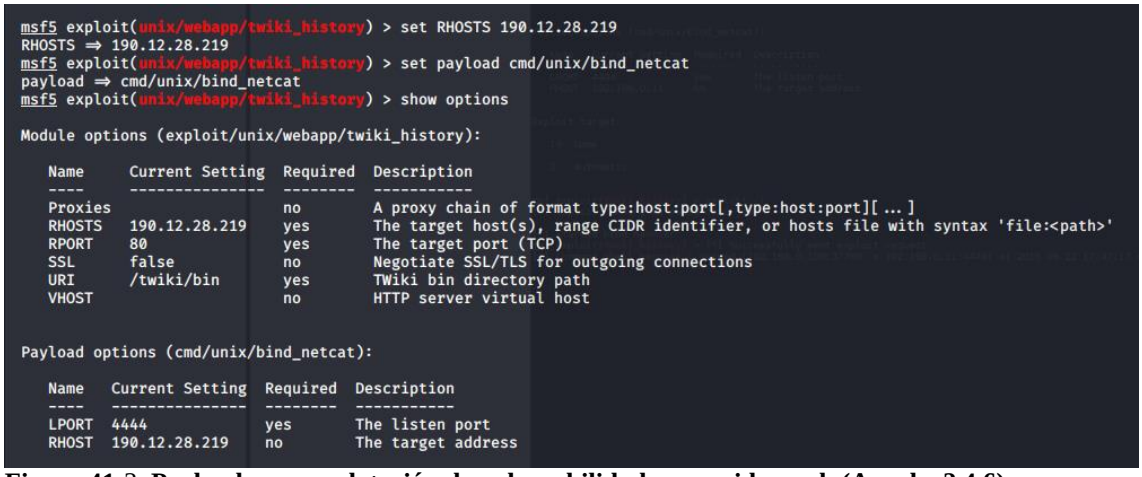


Figura 41-3. **Payload para explotación de vulnerabilidad en servidor web (Apache 2.4.6)**
Elaborado por: Pinango Álvaro, 2020

En la figura presenciada anteriormente se lanzó el ataque permitiendo acceder a la información del servidor como tal, en cuestiones de seguridad simplemente se realizaría una escala de privilegios para obtener información más a fondo del equipo como lo es: configuración ssh, apertura de puertos, denegación de un servicio, o incluso generar diferentes backdoors para mantener la conexión y seguir accediendo a la información.

3.7.3.9 A10-Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)

En cada una de las explotaciones anteriores no existió ninguna intervención por parte de la misma plataforma o agentes de control de la institución, motivo por el cual ninguno de los intentos realizados fue denegado o frustrado y permitió la libre explotación de las debilidades de la plataforma; por ejemplo, ataques como el de fuerza bruta realizado en el caso de A2-Broken Authentication para descifrar las credenciales de acceso se pudieron lograr gracias a que no existió un controlador de intentos de logueo o peticiones masivas realizadas a la plataforma.

Asimismo, los ataques de inundación de peticiones (paquetes) fueron permitidos hasta llegar a la denegación o colapso del servicio de la plataforma, en vista que no existía un control adecuado de peticiones simultáneas por IP o por solicitudes aceptadas.

3.7.4. Fase 4. Generación de informes

Esta etapa consiste en elaborar un plan de seguridad para el aseguramiento de la información que alberga la plataforma, de tal manera que ayude a mejorar significativamente el actual estado de seguridad y pueda preservar la calidad del servicio ofrecido, en dicho plan debe comprender la seriedad de los riesgos emanantes de las vulnerabilidades descubiertas en las fases anteriores, remarcando aquellos puntos en los que la seguridad se había implantado de manera correcta y aquellos que deben ser corregidos.

En vista que el plan será leído tanto por personal a fin a la seguridad informática, así como personal de la alta dirección que comúnmente desconocen de términos técnicos conviene separar el informe en una parte de explicación general y en otra parte más técnica lo que vendría a ser por una parte el informe ejecutivo y el informe técnico.

El punto ideal u objetivo de este tema de investigación específicamente es llegar a establecer las políticas de seguridad para el cumplimiento del plan de seguridad, mismas que consisten en recomendaciones y contramedidas para prevenir estas vulnerabilidades. Las políticas de seguridad son tecnológicas, es decir, de implementación y organizacionales con el fin de mejorar las acciones por parte del personal de la Unidad de Tecnologías y a su vez fomentar una cultura preventiva en los usuarios. En la siguiente sección se procede a redactar esta propuesta.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Presentación de resultados

En este capítulo se detallan los resultados obtenidos en la investigación con los métodos y técnicas planteados, del mismo modo, se realiza la relación con los objetivos y la hipótesis planteada.

4.2. Resultados de la fase 1 (Recopilación de información)

La Tabla 8-4 muestra los dispositivos con los que cuenta la plataforma informática del Cuerpo de Bomberos del Gobierno Autónomo Descentralizado Municipal de Santo Domingo una vez realizado el reconocimiento visual de la infraestructura y del funcionamiento de la misma.

Tabla 8-4. Listado de dispositivos de la plataforma informática

Dispositivo	Detalle	Función
Sitio web	URLs: bomberossantodomingo.gob.ec URLs: cbsd.gob.ec	Página web informativa institucional
Mikrotik WAN	Mikrotik	Administración de servicios de internet para la edificación
Mikrotik LAN	Mikrotik	Firewall
Servidor APP	Servidor de aplicaciones web (Apache, NodeJS) Sistema operativo: CentOS 7 IP: 192.168.1.4 – servicios.cbsd.gob.ec	Plataforma virtual para la atención en línea de la ciudadanía
Servidor APP2	Servidor de aplicaciones web (Apache, NodeJS) Sistema operativo: CentOS 7 IP: 192.168.1.6 – prevención.cbsd.gob.ec	Servidor de respaldo en caso de colapsar el primer servidor; Plataforma virtual para la atención en línea de la ciudadanía
Servidor BDD	Servidor de base de datos (PostgreSQL) Sistema operativo: Windows Server 2008 IP: 192.168.1.3	Servidor de base de datos, alimenta la información a los servidores de aplicaciones

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

En la Tabla 9-4 presenta en resumen los componentes y/o herramientas utilizadas en el desarrollado y despliegue de la plataforma informática, dicha información ha sido entregada por la Unidad de Tecnologías de la institución.

Tabla 9-4. Componentes y/o herramientas de la plataforma informática

Componente	Descripción
Infraestructura	Cliente-Servidor (MVC)
Sistemas operativos	CentOS 7, Windows Server 2008
Lenguajes de programación, diseño y maquetado	PHP, JavaScript, HTML, CSS
Servidores web	Apache, NodeJS
Bases de datos	PostgreSQL
Otras herramientas de desarrollo y despliegue	Git

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

4.3. Resultados de la fase 2 (Identificación de vulnerabilidades)

Mediante las pruebas de escaneo de vulnerabilidades realizadas tomando como base de identificación las 10 vulnerabilidades más críticas descritas en OWASP Top 10 - 2017 se comprobó que la plataforma informática es vulnerable ante los siguientes aspecpectos:

- A1-Injection (Inyección)
- A2-Broken Authentication (Autenticación rota)
- A3-Sensitive Data Exposure (Exposición de datos sensibles)
- A5-Broken Access Control (Pérdida de control de acceso)
- A6-Security Misconfiguration (Control de seguridad incorrecta)
- A7-Cross-Site Scripting (XSS)
- A9-Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)
- A10-Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)

4.4. Resultados de la fase 3 (Explotación de resultados)

Al aplicar la explotación a las 8 vulnerabilidades encontradas con el escaneo de la fase 2 con las herramientas de Metasploit, BurpSuite, Wireshark, SQLmap se identificó que todas pueden ser explotadas, es decir cada una puede ser prevenida.

4.5. Prueba de la hipótesis de investigación

En base a los resultados obtenidos, se comprueba la diferencia entre el nivel de seguridad existente sin un plan de seguridad frente al escenario donde ya se ha implementado un plan de seguridad.

Los escenarios en los que se realizaron las pruebas hacen referencia a la plataforma informática del Cuerpo de Bomberos del GADM-SD con las siguientes consideraciones:

- **Escenario 1**
    - Plataforma informática del CB-GADM-SD en producción
    - Se estableció OWASP Top 10 para la selección de vulnerabilidades a evaluar
- **Escenario 2**
    - Plataforma informática del CB-GADM-SD en producción
    - Se estableció OWASP Top 10 para la selección de vulnerabilidades a evaluar
    - Se implementó un plan de seguridad basado en las normas ISO 27001 para el tratamiento y prevención de vulnerabilidades

Adicionalmente, es preciso mencionar que, posterior al periodo de finalización de la presente investigación, la institución dentro de sus procesos de planificación operativa anual ha realizado la actualización de su proveedor de Internet, motivo por el cual se ha cambiado el Pool de direcciones IPs asignadas para el servicio de Internet, por tanto, las direcciones publicadas en esta investigación han sido reemplazadas para el despliegue de la plataforma informática institucional.

4.5.1. Valoración de la variable independiente

A la variable independiente de la hipótesis "Plan de seguridad" se aplicó la observación como técnica de valoración y poder así validar el cumplimiento del uso de los parámetros planteados para la evaluación de prevención de vulnerabilidades en los escenarios de trabajo.

4.5.1.1 Indicador: Seguridad de la plataforma

Para evaluar la "seguridad de la plataforma" se tomó como referencia el listado de los riesgos más críticos en aplicaciones web establecidos en OWASP Top 10; de dicho listado se seleccionó las vulnerabilidades que hacen referencia a las relacionadas con la arquitectura y herramientas de

despliegue de la plataforma informática del presente caso de estudio, la evaluación se realizó en los escenarios establecidos.

Tabla 10-4. Vulnerabilidades a ser evaluadas en la plataforma informática

Vulnerabilidad detectada de acuerdo a OWASP Top 10-2017
A1-Injection (Inyección de código)
A2-Broken Authentication (Autenticación rota)
A3-Sensitive Data Exposure (Exposición de datos sensibles)
A5-Broken Access Control (Pérdida de control de acceso)
A6 -Security Misconfiguration (Control de seguridad incorrecta)
A7-Cross-Site Scripting (XSS)
A9-Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)
A10-Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

4.5.2. Valoración de la variable dependiente

Para la valoración de las "vulnerabilidades en la plataforma informática" se utilizó el conjunto de herramientas de pruebas de penetración de Kali Linux, entre ellas: Ettercap, Zenmap, SQLmap, BurpSuite; también se trabajó con otras herramientas que permitieron escanear y explotar vulnerabilidades (Wireshark, Vega, Nessus).

4.5.2.1 Indicador: Número de vulnerabilidades escaneadas

Para la obtención del número de vulnerabilidades en este proceso se hizo uso de herramientas y técnicas de detección y explotación de vulnerabilidades, el resultado fue el siguiente:

Tabla 11-4. Vulnerabilidades encontradas en los escenarios de trabajo

Vulnerabilidad detectada de acuerdo a OWASP Top 10-2017	Sin plan de seguridad	Con plan de seguridad
A1-Injection (Inyección de código)	X	
A2-Broken Authentication (Autenticación rota)	X	
A3-Sensitive Data Exposure (Exposición de datos sensibles)	X	X

A5-Broken Access Control (Pérdida de control de acceso)	X	
A6 -Security Misconfiguration (Control de seguridad incorrecta)	X	
A7-Cross-Site Scripting (XSS)	X	
A9-Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)	X	X
A10-Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)	X	
Total	8	2

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

4.5.3. Resultados de indicadores

La medición de los indicadores se realizó en base a las vulnerabilidades encontradas, en la Tabla 15-4 se determina si fue posible la mitigación de la misma después de la aplicación del plan de seguridad propuesto en el presente estudio.

Tabla 12-4. Éxito de mitigación vulnerabilidades detectadas

Vulnerabilidad detectada de acuerdo a OWASP Top 10-2017	SI	NO
A1-Injection (Inyección de código)	X	
A2-Broken Authentication (Autenticación rota)	X	
A3-Sensitive Data Exposure (Exposición de datos sensibles)		X
A5-Broken Access Control (Pérdida de control de acceso)	X	
A6 -Security Misconfiguration (Control de seguridad incorrecta)	X	
A7-Cross-Site Scripting (XSS)	X	
A9-Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)		X
A10-Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)	X	

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

Del mismo modo se determinó que, con la implementación del plan de seguridad se previene las vulnerabilidades que pondrían comprometer la confidencialidad, integridad y disponibilidad de la información de la plataforma informática del CB-GADM-SD, es decir, se cumple satisfactoriamente con éxito.

En la tabla y las figuras (Figura 42-4 y Figura 43-4) que se presentan a continuación se puede comprobar gráfica y estadísticamente el nivel de mejora de seguridad de la plataforma informática con la implementación del plan de seguridad propuesto.

Tabla 13-4. Mitigación de vulnerabilidades encontradas

Parámetro a evaluar	Vulnerabilidades encontradas	Vulnerabilidad de la plataforma
Plataforma informática sin plan de seguridad	8	100%
Plataforma informática con plan de seguridad	2	25%

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

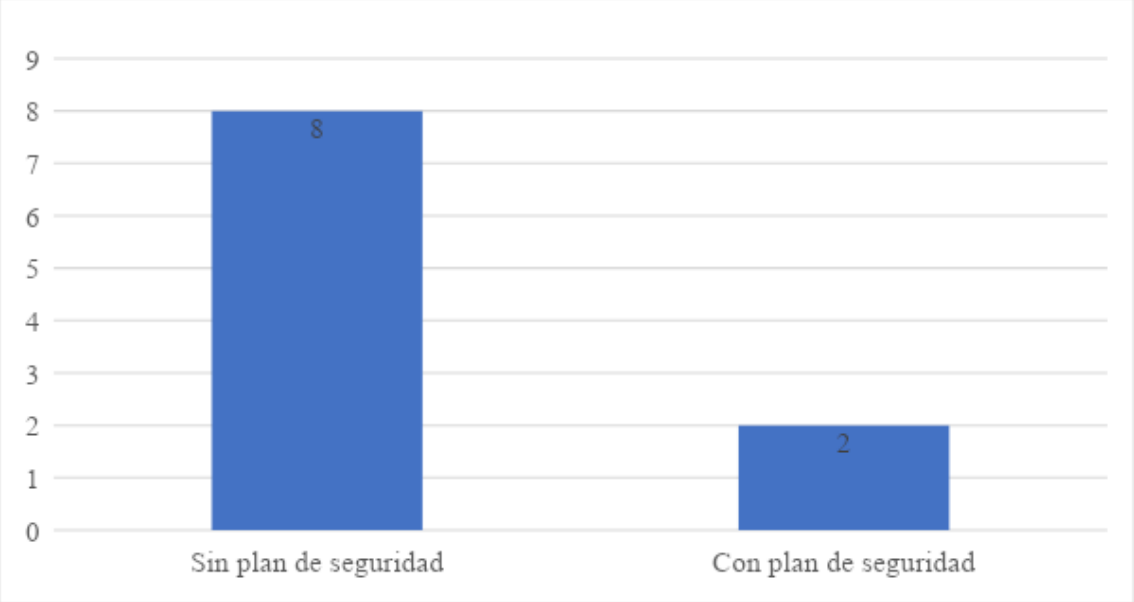


Gráfico 1-4. Número de vulnerabilidades encontradas en la plataforma informática
Elaborado por: Pinango Álvaro, 2020

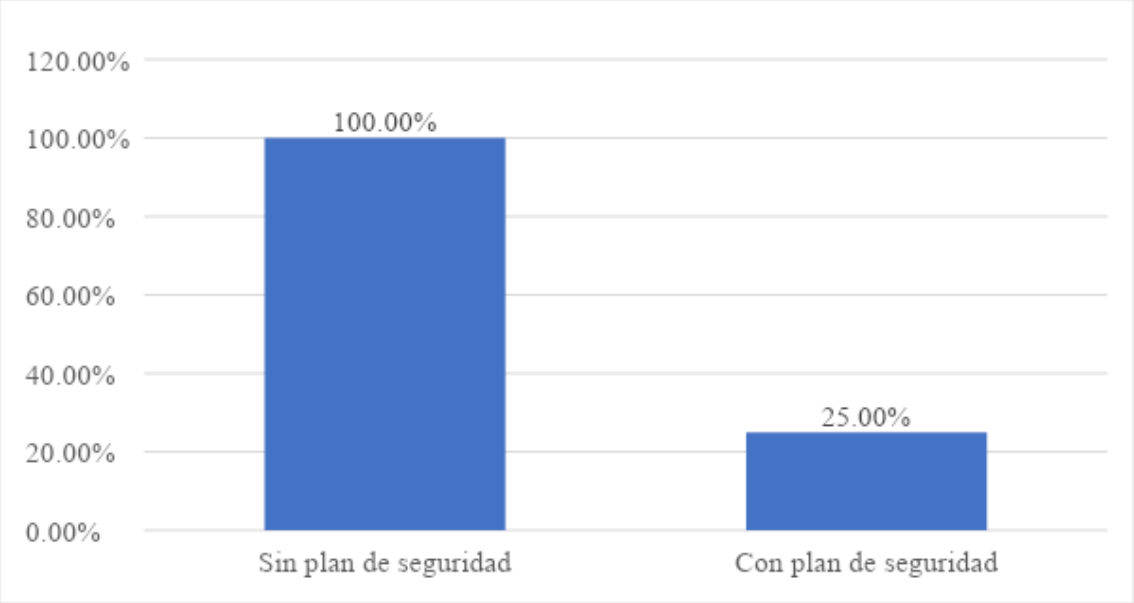


Gráfico 2-4. **Vulnerabilidad de la plataforma informática con y sin plan de seguridad**
Elaborado por: Pinango Álvaro, 2020

4.5.4. Análisis e interpretación de resultados

De los datos obtenidos, el porcentaje de aplicabilidad se calcula como valor de 8 correspondiente al 100%, puesto que se indica los parámetros en su totalidad a evaluar. Por lo tanto, la valoración obtenida en el escaneo de vulnerabilidades dentro del escenario de trabajo sin plan de seguridad es de 8 correspondiente al 100% de vulnerabilidad; mientras que, la valoración en el mismo escenario aplicado el plan de seguridad es de 2 correspondiente al 25% de vulnerabilidad. Por lo tanto, se puede deducir que, al aplicar el plan de seguridad propuesto se mejora significativamente un 75% el nivel de seguridad de la plataforma informática del CB-GADM-SD.

4.6. Comprobación estadística de la hipótesis

En la comprobación de la hipótesis general "La implementación del plan de seguridad propuesto prevendrá la presencia de vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo", se utilizó estadística referencial aplicando la prueba Chi-Cuadrado (x^2).

Con los datos previamente obtenidos se definen la Hipótesis de Investigación (Hi) y la Hipótesis Nula (Ho):

> **Hi:** El plan de seguridad **sí** prevendrá la presencia de vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo.

Ho: El plan de seguridad **no** prevendrá la presencia de vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo.

La tabla que se presenta a continuación, contiene las frecuencias de valores encontrados, de dichos valores parte el cálculo de la prueba de comprobación de la hipótesis.

Tabla 14-4. Tabla de frecuencias de valores encontrados

Parámetro a evaluar	Escenario 1 (Sin plan de seguridad)	Escenario 2 (Con plan de seguridad)	Total
Vulnerabilidades encontradas	8	2	10
Vulnerabilidades solventadas	0	6	6
Total	8	8	16

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

Aplicando la siguiente fórmula a cada valor de la Tabla 17-4 se obtienen los valores de la matriz de frecuencia esperadas como se plantea en la Tabla 18-4.

$$Fe = \frac{(total\ columna\ * total\ fila)}{(suma\ total)}$$

Tabla 15-4. Tabla de valores de frecuencias esperadas

Parámetro a evaluar	Escenario 1 (Sin plan de seguridad)	Escenario 2 (Con plan de seguridad)	Total
Vulnerabilidades encontradas	5	5	10
Vulnerabilidades solventadas	3	3	6
Total	8	8	16

Fuente: Investigación
Elaborado por: Pinango Álvaro, 2020

A continuación, se calcula el valor de x^2 mediante la siguiente fórmula

$$x^2 = \sum \frac{(FO - FE)^2}{FE}$$

Dónde:

F0: Frecuencia observada por celda

FE: Frecuencia esperada por celda

$$x^2 = \frac{(8-5)^2}{5} + \frac{(0-3)^2}{3} + \frac{(2-5)^2}{5} + \frac{(6-3)^2}{3}$$

$$x^2 = 1.8 + 3 + 1.8 + 3$$

$$x^2 = 9.6$$

El siguiente paso a seguir es el cálculo de los grados de libertad

$$v = (r-1) * (k-1)$$

Dónde:

r: número de filas

k: número de columnas

$$v = (2-1) * (2-1)$$

$$v = 1$$

En base a la tabla de la distribución de Chi-Cuadrado, y determinando el valor de significancia de 0.05% obtenemos el punto crítico con 1 como valor de grados de libertad.

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, ν = Grados de Libertad

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

Figura 42-4. **Distribución Chi Cuadrado**
Fuente: Investigación

$$x^2 crítico = 3.8415$$

Dado los datos anteriores **Ho** debe ser aceptada si sucede el siguiente condicionante

$$x^2 calculado \leq x^2 crítico$$

Caso contrario se rechaza **Ho** y se acepta **Hi**

Con las operaciones anteriores se obtuvo los siguientes datos:

$x^2 = 9.6$

$$x^2 crítico = 3.8415$$

Por lo tanto, se puede aplicar el criterio de decisión con el siguiente gráfico.

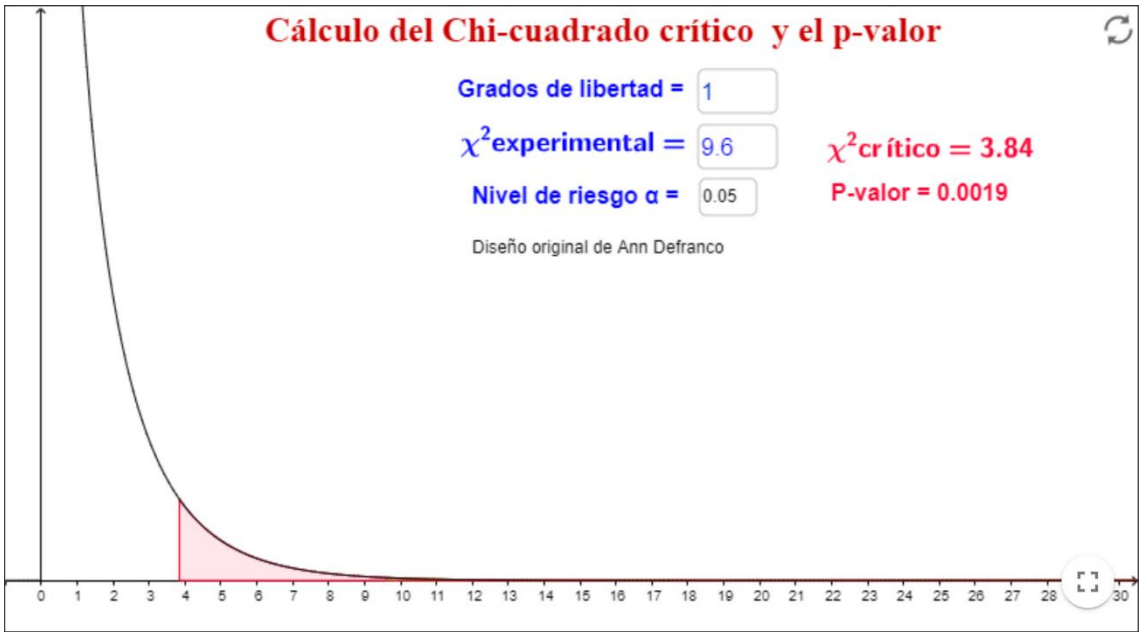


Gráfico 3-4. **Chi-Cuadrado y criterios de Aceptación de Hi**
Elaborado por: Pinango Álvaro, 2020

4.7. Interpretación y análisis

En consecuencia, con los datos obtenidos y como se aprecia en la gráfica se concluye que se rechaza la Hipótesis nula (**Ho**) y se acepta la Hipótesis alternativa (**Hi**) con un nivel de confianza del 95% y un nivel de significancia de 5%.

CAPÍTULO V

5. PROPUESTA

En la actualidad, la seguridad informática se ha tornado como un punto imprescindible para el correcto desarrollo de las plataformas informáticas y sus recursos, para ello, es importante la formación del personal de tecnologías en temas de seguridad y ciberseguridad ya sea en entidades públicas y/o privadas. Fomentar esta cultura informática en las organizaciones logrará que la Unidad de Tecnologías de esta institución tome decisiones conjuntamente con la Dirección en beneficio de los objetivos de la organización y optimizar así el rendimiento de los servicios ofrecidos en pro de la ciudadanía y consigo misma.

Con la presente investigación se determinó que la plataforma informática no era segura para albergar la información de sus usuarios, por lo tanto, para contrarrestar las falencias encontradas, es necesario aplicar los correctivos que se plantean en este capítulo, puesto que, el principal enfoque de la plataforma informática del Cuerpo de Bomberos es, brindar un servicio de calidad a la ciudadanía y mantener la confidencialidad, integridad y disponibilidad de la misma.

En este capítulo se enfoca en las acciones que debe tomar la organización como un solo equipo de trabajo, unificando sus procesos y procedimiento en una sola tarea conjunta. Se establecen las políticas de seguridad que se basan en la configuración adecuada de equipos, las acciones necesarias a tomar frente a una determinada situación, así como los procedimientos necesarios para llevar un control de vida de los equipos, abarcando así tanto el ámbito de la institución, así como también la infraestructura que mantiene la misma.

5.1. Plan de seguridad para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo empleando las normas ISO 27001

5.1.1. Objetivo

Brindar estrategias y políticas de seguridad para prevenir la aparición de vulnerabilidades que afecten la seguridad de la información y el mejoramiento continuo de la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo.

5.1.2. Alcance

El presente Plan de Seguridad fue aplicado en la plataforma informática en el Cuerpo de Bomberos del GAD Municipal de Santo Domingo, mismo que se encuentra situado en la ciudad de Santo Domingo, en la Av. Jacinto Cortéz y Jorge Icaza de la cooperativa Santa Marta.

Cuyo cumplimiento es de carácter obligatorio para toda la organización, incluyendo a las demás estaciones y subestaciones del Cuerpo de Bomberos del GAD Municipal de Santo Domingo, a las cuales acceden a la plataforma informática mediante los servicios web que se encuentran siempre en línea, la disponibilidad y el buen funcionamiento de dicha plataforma estará siempre relacionada al buen uso que se dé a la misma.

5.1.3. Roles y responsabilidades

Es importante mencionar que las responsabilidades referentes a la seguridad de información son distribuidas en toda la organización, en ese sentido existen roles adicionales que recaen en los propietarios y los custodios de la información. Los propietarios de la información deben verificar su integridad y velar para que se mantenga su disponibilidad y confidencialidad.

Los custodios de información son responsables de monitorear el cumplimiento de las actividades encargadas, mientras que, la Unidad de Tecnologías debe monitorear el cumplimiento de políticas de seguridad y el cumplimiento adecuado de los procesos definidos para mantener la seguridad.

A continuación, se detallan los roles y responsabilidades en la administración de seguridad de información, tomando en cuenta a las direcciones o unidades de mayor control de la información:

- **Dirección General (Alta Dirección)**
    - Toma de decisiones en base a los análisis expuestos por las demás unidades o direcciones.
- **Dirección de Talento Humano**
    - Evalúa al personal enrolado con la organización y procede a la firma de un acuerdo de confidencialidad y no divulgación de la información.
    - Asignación de medidas correctivas disciplinarias en caso de incumplimiento de normas o políticas de seguridad.
- **Dirección Administrativa**

- Administra los recursos de la organización y el control de calidad de los procesos relacionados con la Unidades de Tecnologías y Control de bienes.

- **Control de bienes**

  - Verifica que cada activo de información haya sido asignado a un custodio y que este procedimiento quede debidamente documentado.

- **Unidad de tecnologías**

  - Establece y documenta las responsabilidades de la organización en cuanto a seguridad de la información.

  - Comunica aspectos básicos de seguridad de información a los funcionarios.

  - Desarrolla controles de seguridad para las tecnologías que utiliza la organización.

  - Realiza una evaluación periódica de las vulnerabilidades de los sistemas que conforman la plataforma informática.

  - Administra programas de clasificación de activos de información, incluyendo la identificación de los propietarios de las aplicaciones y datos.

  - Coordina las funciones relacionadas a seguridad como: seguridad física, seguridad de personal y seguridad de información almacenada en medios no electrónicos.

  - Elabora y mantiene un registro de revisiones periódicas de la configuración de accesos en los sistemas de la institución.

  - Protege la integridad de los bienes informáticos supervisando el trabajo de los funcionarios.

  - Mantiene las políticas y estándares de seguridad de la información de la organización, además de monitorear su cumplimiento.

  - Cumple lo establecido entre las políticas y medidas de seguridad respecto a los respaldos del sistema operativo y de las aplicaciones, así como de los datos.

  - Garantiza que los servicios implementados sean utilizados para los fines que fueron creados.

- Comunica a la alta dirección los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.

- Activa los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.

- Controla de forma sistemática la integridad del software que se encuentra instalado en los servidores., además del acceso a los sistemas, aplicaciones y bases de datos.

- Detecta posibles vulnerabilidades en los sistemas y aplicaciones bajo su responsabilidad y propone acciones para su solución.

- **Propietarios de información**

  Se establece como propietarios de información a los responsables de las unidades o direcciones de la institución, los cuales, son responsables de la información generada y utilizada en las operaciones de su unidad. Cada unidad debe ser consciente de los riesgos por el incumplimiento de dichas normas. Sus responsabilidades son:

  - Asignar los niveles iniciales de clasificación de información; cada funcionario es responsable de la información que gestiona en el puesto de trabajo.

  - Revisar periódicamente la clasificación de la información con el propósito de verificar que cumpla con los requerimientos de la organización.

  - Verificar periódicamente la integridad y coherencia de la información que se encuentra bajo su responsabilidad.

  - Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.

  - Revisar los niveles de acceso a los sistemas que se encuentran a su cargo.

  - Determinar la viabilidad de realizar copias de respaldo para su información.

  - Determinar las acciones indicadas en caso de violaciones de seguridad detectadas en su unidad.

- **Otros usuarios**

Son aquellas personas que hacen uso de la plataforma informática institucional como parte de su trabajo diario, sus responsabilidades son definidas a continuación:

- Mantener la confidencialidad de las credenciales de acceso a los sistemas usados.
- Reportar incidentes o violaciones de la seguridad presenciados en la plataforma.
- Registrar únicamente información necesaria y adecuada a los sistemas.
- Acatar las políticas de seguridad establecidas.
- Emplear la información exclusivamente para los propósitos autorizados.

5.1.4. Organización del área de seguridad informática propuesta

Es necesaria la existencia del área organizacional con el fin de administrar la seguridad de la información, puesto que la presente plataforma informática alberga datos sensibles y confidenciales de la ciudadanía y de sus funcionarios, la misma que es ingresada con fines institucionales para acceder a los servicios brindados por la institución.

Considerando la falta de recursos con el perfil requerido que puedan ser rápidamente reasignados, el proceso de entendimiento y asimilación de las responsabilidades, los roles definidos correspondientes al área de seguridad informática y la necesidad de implementar un esquema adecuado de seguridad, se propone un Plan de Seguridad para prevenir las vulnerabilidades en la plataforma informática del Cuerpo de Bomberos del GADM-SD, de esta manera se pretende mantener a salvo la información que ingresan los usuarios, del mismo modo, salvaguardar la información en caso de desastres y conseguir la continuidad del servicio completo. Este plan de seguridad brindará los siguientes beneficios:

- Prevención de vulnerabilidades en la plataforma informática.
- Actualización de las herramientas que conforman la plataforma informática.
- Definir roles y responsabilidades de las actividades para salvaguardar la información.

5.1.5. Análisis y evaluación de riesgos: identificación de amenazas, consecuencias y criticidad

El análisis y evaluación de riesgos y sus consecuencias se establece de acuerdo a la metodología de evaluación de riesgos de ISO 27001.

5.1.5.1 Recogida y preparación de la información

Con el propósito de obtener un adecuado entendimiento de la implicancia que tiene el uso de tecnologías, las amenazas y vulnerabilidades, así como las iniciativas del negocio sobre la prevención de vulnerabilidades de la Plataforma Informática del Cuerpo de Bomberos del GADM-SD, además, contando con la debida autorización de la Dirección General, se efectuaron pruebas de penetración a dicha plataforma con el fin de evaluar el nivel de seguridad con el que cuenta antes de la implementación del plan de seguridad propuesto.

Los activos del caso de estudio se clasifican de la siguiente manera:

- Equipos de la red interna de trabajo
    - Computadores de escritorio (estaciones de trabajo), equipos portátiles (laptops).
- Equipos que conforman la plataforma informática
    - Servidores de aplicaciones, servidor de base de datos, router de salida

5.1.5.2 Identificación y clasificación de las amenazas

Las amenazas más importantes a considerar de acuerdo al impacto que pudieran tener sobre la caída del servicio de la plataforma informática del Cuerpo de Bomberos del GADM-SD son:

- Pérdida de disponibilidad del servicio.
- Acceso no autorizado a la red, tanto producto de un ataque externo como interno.
- La sustracción, alteración o pérdida de datos, incluso la fuga de información clasificada.
- La introducción de programas malignos desde la red interna: Al no contar con una cuenta de usuario estándar en lugar de una de administrador, los funcionarios de la institución pueden instalar aplicaciones de su conveniencia, incluso que no tengan que ver con las labores diarias de su función.
- El empleo inadecuado de las tecnologías y sus servicios: Mal uso de los recursos de la institución, uso de servidores de archivos como almacenamiento de datos personales, descarga de archivos no relevantes, etc.

5.1.5.3 Identificación y estimación de las vulnerabilidades

En esta sección se presentan las amenazas identificadas, así como las implicaciones de seguridad que ocasionaría cada riesgo y los estándares de seguridad necesarias para prevenir cada vulnerabilidad.

Tabla 16-5. Identificación de vulnerabilidades y sus consecuencias

Vulnerabilidad	Implicación de seguridad
Injection (Inyección de código)	La inyección de código malicioso puede ocasionar la pérdida de datos, corrupción o divulgación de información a partes no autorizadas, pérdida de responsabilidad o denegación de acceso. También puede conducir a la adquisición completa del equipo.
Broken Authentication (Autenticación rota)	Los atacantes obtienen acceso a cuentas de usuarios privilegiados para comprometer el sistema. Dependiendo del dominio de la aplicación, esto puede permitir el lavado de dinero, el fraude de la seguridad social y el robo de identidad, o revelar información altamente confidencial legalmente protegida.
Sensitive Data Exposure (Exposición de datos sensibles)	Con frecuencia se compromete todos los datos que deberían estar protegidos. Por lo general, esta información incluye datos de información personal confidencial, como registros de salud, credenciales, datos personales y cuentas bancarias, entre otras.
Broken Access Control (Pérdida de control de acceso)	Los atacantes actúan como usuarios privilegiados para poder crear, acceder, actualizar o eliminar registros, entre otras funciones de carácter perjudicial. Fácilmente se podría comprometer datos privilegiados de un sistema informático.
Security Misconfiguration (Control de seguridad incorrecta)	Los atacantes se valen de errores de configuraciones o configuraciones por defecto para ganar acceso no autorizado a algunos datos del sistema o funcionalidad, eventualmente estos resultan en un compromiso completo del sistema.
Cross-Site Scripting (XSS)	Los ataques XSS típicos incluyen robo de sesión, reemplazo o desfiguración de DOM (como paneles de inicio de sesión), ataques contra navegadores, descargar software malicioso, registro de claves y otros ataques del lado del cliente.
Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)	Si bien, algunas vulnerabilidades conocidas provocan solo impactos menores, algunas de las violaciones más grandes hasta la fecha se han basado en la explotación de vulnerabilidades conocidas en los componentes. Puesto que comunidades que se dedican a la explotación de componentes están en constante búsqueda de nuevas vulnerabilidades por más nueva que sean las herramientas utilizadas.
Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)	Los ataques más exitosos comienzan con el sondeo de vulnerabilidades. Permitir que tales sondas continúen puede aumentar la probabilidad de una explotación exitosa a casi el 100%.

Elaborado por: Pinango Álvaro, 2020

En la sección que se plantea a continuación, se establecen las posibles soluciones que se deben emplear para llegar a la prevención de dichas vulnerabilidades en la plataforma.

Tabla 17-5. Medidas de seguridad para prevenir la explotación de las vulnerabilidades

Vulnerabilidad	**Medida de seguridad a aplicar**
Injection (Inyección de código)	• Implementar APIs seguras, que eviten el uso del intérprete por completo. • Implementar herramientas de mapeo relacional de objetos (ORM) para consultas. • Generar consultas indexadas: hacer uso operadores como LIMIT y otros controles SQL para evitar la divulgación masiva de registros en caso de inyecciones SQL.
Broken Authentication (Autenticación rota)	• Evitar el uso de credenciales que tengan relación directa con datos personales como: números de identificación, fechas de nacimiento, nombres o apellidos, etc. • Implementar algoritmos de comprobación de contraseñas débiles para establecer las credenciales de acceso. • Forzar la actualización periódica de contraseña para todos los usuarios. • Limitar los intentos fallidos de inicio de sesión, registrar las fallas y dar aviso a los administradores cuando se detecten el relleno de credenciales, la fuerza bruta u otros ataques. • Administrar las sesiones de usuario del lado del servidor, además generar IDs de sesión aleatorios en cada logueo. • Evitar el envío de IDs de sesión y otros parámetros en la URL.
Sensitive Data Exposure (Exposición de datos sensibles)	• Identificar los datos que se consideren sensibles de acuerdo a reglas del negocio de la institución. • No requerir información confidencial no sea necesaria. • Implementar cifrado de datos. • Cifrar todos los datos en tránsito con protocolos seguros como TLS con cifrados de secreto directo perfecto (PFS), priorización de cifrado por parte del servidor y parámetros seguros. Aplicar el cifrado mediante directivas como HTTPS. • Deshabilitar el almacenamiento en caché para formularios con datos confidenciales. • Utilizar funciones de hashing para almacenamiento de contraseñas.
Broken Access Control (Pérdida de control de acceso)	• Restringir el acceso a directorios y recursos que no sean de carácter público. • Implementar mecanismos de control de acceso en toda la aplicación. • Validar las rutas de navegación en base a perfiles y roles de usuario. • Deshabilitar la lista del directorio del servidor web y asegúrese de no exponer los metadatos y archivos de respaldo no estén presentes en las raíces web. • Registrar las fallas de control de acceso y alertar a los administradores. • Limitar de velocidad API y acceso al controlador para minimizar el daño de las herramientas de ataque automatizado.
Security Misconfiguration (Control de seguridad incorrecta)	• Los entornos de desarrollo, control de calidad y producción deben configurarse de manera idéntica, con diferentes credenciales utilizadas en cada entorno. • Eliminar funciones y marcos que no se estén utilizando. • Programar tareas para revisar y actualizar las configuraciones para todas las notas de seguridad, actualizaciones y parches. • Verificar la efectividad de las configuraciones en todos los entornos.
Cross-Site Scripting (XSS)	• Usar marcos que escapan automáticamente a XSS por diseño. • Rechazar los datos de solicitud HTTP no confiables basados en el contexto en la salida HTML (cuerpo, atributo, JavaScript, CSS o URL). • Aplicar técnicas de escape sensibles al contexto similares a las API del navegador. • Habilitar una Política de seguridad de contenido (CSP) como un control de mitigación de defensa en profundidad contra XSS.

Using Components with Known Vulnerabilities (Uso de componentes con vulnerabilidades conocidas)	• Eliminar dependencias, componentes, archivos y documentación innecesaria. • Hacer un inventario continuo de las versiones de los componentes y dependencias de la plataforma. • Supervisar continuamente las fuentes como CVE para detectar vulnerabilidades, utilizar herramientas de análisis de software para automatizar el proceso. • Consultar sitios que permitan suscribirse a las alertas por correo electrónico para conocer las vulnerabilidades de seguridad de los componentes que utiliza. • Implementar componentes de fuentes oficiales a través de enlaces seguros. • Supervisar las bibliotecas y los componentes que no están mantenidos o que no crean parches de seguridad para versiones anteriores.
Insufficient Logging&Monitoring (Registro y monitoreo insuficientes)	• Establecer un monitoreo efectivo de modo que las actividades sospechosas sean detectadas y respondidas de manera oportuna. • Asegurar que las transacciones de alto valor tengan una pista de auditoría con controles de integridad para evitar alteraciones o supresiones, como tablas de base de datos de solo agregar o similares. • Registrar todas las fallas de inicio de sesión, control de acceso y validación de entrada del lado del servidor e identificar cuentas sospechosas o maliciosas, y almacenarlas hasta realizar un análisis forense retrasado. • Establecer un plan de respuesta y recuperación de incidentes.

Elaborado por: Pinango Álvaro, 2020

5.1.6. Políticas de seguridad

La base de las políticas de seguridad se fundamentará bajo los siguientes principios:

- La Dirección General del Cuerpo de Bomberos del GADM-SD será quien apruebe la propuesta encaminada a mejorar el sistema de seguridad informática.

- Para acceder a las tecnologías con las que cuenta la institución el personal tiene que contar con una aprobación en cada caso, del mismo modo, debe estar previamente preparado en los aspectos relativos a la seguridad informática.

- Para el uso y acceso de los sistemas y los recursos de información se establecerán procedimientos en los que se especifique quién y cómo será su acceso; de igual manera, sus derechos, privilegios y suspensión de acceso al sistema.

- Se asignará una cuanta institucional a cada funcionario de la institución, la misma que deberá ser usada exclusivamente para fines laborales.

- En el caso de detectar una violación de seguridad informática, se deberá informar de forma inmediata al feje inmediato y este a su vez a la Unidad de Tecnologías, quienes se encargarán de crear una comisión que analice los sucesos y brinde las medidas correctivas necesarias u oportunas.

- El personal de tecnologías se encarga de la protección de la información y están en la obligación de informar cualquier incidente o violación ocasionado a su jefe inmediato.

5.1.6.1 Control de los bienes informáticos

Medidas generales:

- Los bienes informáticos deben estar bajo la custodia de un funcionario de la institución, este proceso será documentado bajo un acta realizada por el responsable de Control de Bienes (Anexo B. Acta entrega recepción de bienes informáticos).

- Cada ordenador contará con un expediente técnico donde se registrarán todos los cambios que ocurran con el equipo (Anexo E. Hoja de vida de los equipos informáticos y Anexo F. Expediente técnico de bienes informáticos).

Procedimiento No 1: Alta de bienes informáticos para su uso (Asignación a un custodio)

1. Realiza controles sobre los bienes informáticos que se encuentran en cada departamento según el inventario de control de bienes.

   Responsable: Control de bienes

2. Elabora un informe con los resultados de cada control y ponerlo en conocimiento de la dirección del centro.

   Responsable: Control de bienes

3. Notifica a la Unidad de Tecnologías la incorporación de cualquier bien informático a los departamentos.

   Responsable: Responsable de la unidad o dirección

4. Garantiza que la ubicación donde se encuentre los bienes informáticos cuente con las medidas de protección física requeridas.

   Responsable: Dirección Administrativa

5. Instala el software autorizado a utilizar en el área a la que fue asignado el bien informático, teniendo en cuenta el software autorizado a instalarse en los bienes informáticos (Anexo C. Listado de software autorizado).

   Responsable: Unidad de tecnologías

6. Actualizar los sistemas informáticos de la entidad

   Responsable: Unidad de Tecnologías

7. Confeccionar el expediente técnico del bien informático

   Responsable: Unidad de Tecnologías

8. Firma del acta de responsabilidad material que incluye el expediente técnico del bien informático.

   Responsable: Custodio del bien informático

9. Capacitar al personal encargado de la operación y protección del bien informático en materia de seguridad informática.

   Responsable: Unidad de Tecnologías

10. Chequear periódicamente el cumplimiento de este procedimiento.

    Responsable: Unidad de Tecnologías

Procedimiento No 2: Asignación y control de bienes informáticos portátiles

1. Solicita por escrito a la Dirección Administrativa la asignación del bien requerido

   Responsable: Responsable de unidad o dirección

2. Una vez aprobada la solicitud, se notifica a Control de Bienes para que proceda con el descargo y asignación del equipo.

   Responsable: Dirección Administrativa

3. Prepara el bien informático con el software autorizado necesario para su uso.

   Responsable: Unidad de Tecnologías.

4. Entrega el equipo al funcionario que hará uso del mismo, dejando constancia en el acta entrega del expediente técnico del que se confecciona posterior a su entrega (Anexo F. Expediente técnico de bienes informáticos).

   Responsable: Unidad de Tecnologías

5. Solicita por escrito mediante un informe la autorización a la Dirección Administrativa, para la entrada y salida de la institución.

   Responsable: Funcionario

6. Evalúa y autoriza el uso del bien informático fuera de la institución.

   Responsable: Dirección Administrativa

7. Garantiza en el acceso principal de la institución que la entrada y salida de computadoras portátiles se realice por el personal autorizado (Anexo D. Registro de entrada y salida de bienes informáticos).

   Responsable: Responsable de seguridad

8. De ser necesaria la entrada de una computadora portátil ajena a la institución por cuestiones de trabajo, solicita la autorización temporal al jefe inmediato.

   Responsable: Funcionario

9. Conserva por un periodo no menor a un año las autorizaciones escritas para la entrada y salida de los equipos portátiles.

   Responsable: Unidad de Tecnologías

10. Actualiza el registro de usuarios autorizados a utilizar las portátiles fuera de la institución.

    Responsable: Unidad de Tecnologías

11. Revisa periódicamente que el registro de usuarios autorizados a utilizar las portátiles fuera de la institución se encuentre debidamente actualizado.

    Responsable: Responsable de seguridad

12. Chequea periódicamente el cumplimiento de este procedimiento.

    Responsable: Dirección Administrativa

5.1.6.2 Del personal

Medidas generales:

- En el proceso de selección del personal que se incorpora a la institución, en caso que su trabajo se vincule con las tecnologías informáticas, se incluirá una valoración de su nivel de preparación.

- La Dirección de Talento Humanos será la responsable de la valoración de la preparación de cada funcionario. Debe quedar documentado el resultado de esta evaluación, así como el plan de capacitación en caso que se requiera.

- La Dirección de Talento Humanos garantiza que en el expediente laboral de cada trabajador que se vincula con las tecnologías informáticas se incluya.

Procedimiento No 3: Selección, preparación y responsabilidad del personal respecto a la Seguridad Informática.

Procedimiento No 4: Otorgar/Retirar acceso de personas a las Tecnologías de Información (dominio, correo, aplicaciones, etc).

Procedimiento No 5: Otorgar/Retirar acceso a los sistemas informáticas de la institución.

Procedimiento No 6: Otorgar/Retirar acceso de usuarios a otras aplicaciones y servicios instalados.

5.1.6.3 Seguridad física y ambiental

Medidas generales:

- El equipo que cause baja o sea destinado para otras funciones será objeto de revisión por parte de la Unidad de Tecnologías, con el fin de evitar que su información sea de conocimiento de otros usuarios (Anexo G. Ficha técnica para el registro de incidencias).

- Los dispositivos de almacenamiento que contengan información clasificada se destruirán físicamente o serán detenidos por la Unidad de Tecnologías según sea tomada la decisión por la Dirección.

- Para lograr la baja de los bienes informáticos se creará una comisión presidida por el responsable de la Unidad de Tecnologías quien decidirá el destino final de los equipos (Anexo H. Resolución de la comisión para la baja de bienes).

Medidas generales para todas las áreas con tecnologías informáticas:

- Los tomacorrientes tendrán señalizado el tipo de voltaje que suministran para evitar accidentes o incendios.

- Los usuarios antes de conectar o desconectar los equipos de la red eléctrica chequearán que estos estén apagados.

- Contar con fuentes de respaldo de energía y estabilizadores de voltaje para cada computadora.

- En el caso de las áreas donde se procesan informaciones clasificadas se tendrá en cuenta la posición del equipamiento, garantizando que las computadoras estén situadas de forma tal que no sea visible la información del monitor.

Medidas para el ahorro de energía en todas las estaciones de trabajo:

- Activar el modo de bajo consumo o configurar la opción de ahorro para el monitor, disco duro e inactividad del PC. Se recomienda entre cinco y diez minutos para el monitor y para el disco duro entre l5 y 30 minutos para la opción inactividad del PC.

- Habilitar el modo de hibernación. Se recomienda seleccionar como rango de tiempo para pasar al modo de hibernación un tiempo no menor de dos horas y no mayor de 4 horas.

- Asegurarse de apagar los equipos y reguladores o ups de las estaciones de trabajo al fin de la jornada laboral.

Medidas para el mantenimiento y reparación de las tecnologías informáticas:

- Las reparaciones menores y los mantenimientos se realizan por la Unidad de Tecnologías y las reparaciones mayores por entidades contratadas (Anexo E. Hoja de vida de los equipos informáticos).

- Siempre que se realice el mantenimiento o la reparación de un equipo en la propia entidad se hará en presencia de una persona del área respectiva. Si el equipo contiene información clasificada y/o limitada debe estar presente el custodio del mismo.

- En caso de que sea necesario el traslado de un equipo fuera de la entidad, deberá reflejarse el movimiento del medio básico, además de actualizar los controles internos que indiquen el lugar donde se encontrará el equipo, su tiempo de permanencia en el taller y el técnico encargado de la reparación.

- Si se trata de una máquina con información sensible, la Unidad de Tecnologías se asegurará que antes de extraerla se retire el disco duro del equipo. Si no es posible su extracción, la información debe ser guardada en otro soporte y borrada físicamente del disco antes de su salida.

Procedimiento No 7: Baja de los bienes informáticos

1. Definir el equipo informático al que se dará de baja.
2. Recoger el equipo informático del área donde se encuentra y trasladarlo a la Unidad de Tecnologías.
3. Solicitar informe técnico de Control de Bienes.

   Responsable: Unidad de Tecnologías
4. Entrega el informe técnico del equipo.

Responsable: Control de Bienes

5. Una copia del informe va para Dirección Financiera y otra la guarda la Unidad de Tecnologías.
6. Da de baja al equipo informático de los activos fijos tangibles en base al informe técnico de la comisión (Anexo H. Resolución de la comisión para la baja de bienes).

   Responsable: Control de Bienes
7. Desactivación del equipo, separando las partes reciclables.
8. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

Procedimiento No 8: Bajas de los bienes informáticos que contengan Información Oficial Clasificada (I.O.C).

1. Revisar el equipamiento propuesto para baja.

   Responsable: Unidad de Tecnologías
2. Solicitar el informe técnico de baja a la comisión para seguir con el procedimiento.

   Responsable: Unidad de Tecnologías
9. Entrega el informe técnico del equipo.

   Responsable: Control de Bienes
3. Borra la información de los bienes informáticos con información oficial clasificada con alguna herramienta de borrado seguro.

   Responsable: Unidad de Tecnologías
4. Registrar en el expediente la baja de la I.O.C almacenada en el bien informático (Anexo I. Expediente de eliminación de Información Oficialmente Clasificada (I.O.C)).

   Responsable: Unidad de Tecnologías
5. Aplicar Procedimiento No. 7: Bajas de los bienes informáticos.

   Responsable: Unidad de Tecnologías
6. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

Procedimiento No 9: Mantenimiento a equipos

1. Se les da mantenimientos a los equipos al menos una vez al año.
2. Registra en el expediente técnico del equipo la fecha del mantenimiento (Anexo E. Hoja de vida de los equipos informáticos).
3. La Unidad de Tecnologías genera la conformidad de los equipos a los que se les dio mantenimiento.

   Responsable: Unidad de Tecnologías
4. Registrar la constancia del mantenimiento realizado en la hoja de vida del equipo.
5. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

5.1.6.4 Desarrollo de software seguro

Medidas generales:

- En el proceso de desarrollo de software para la ceración de nuevos módulos o la modificación de los mismos, los desarrolladores deberán realizar un estudio sistemático de las vulnerabilidades que se podrán generar a raíz de la inserción de metodologías de trabajo, lenguajes de programación empleados, o bases de datos usadas.

- Los componentes implementados para el despliegue de la plataforma deberán ser únicamente provenientes de fuentes confiables.

- Se realizarán las pruebas respectivas antes de hacer deploy del software desarrollado, del mismo modo en la adquisición de nuevas herramientas de software se deberán realizar las pruebas necesarias en la puesta en marcha con el fin de que el proveedor de la solución antes de finalizar la adquisición.

Procedimiento No 10: Prevenir inyecciones sql

1. Se mantendrá por separado los datos de los comandos y las consultas.
2. Se debe implementar una herramienta de Mapeo Relacional de Objetos (ORMs) con el objetivo de evitar el uso del intérprete por completo y proporcionar una interfaz parametrizada.
3. Realizar validaciones de entradas de datos en el servidor. Evitar en lo posible el uso de caracteres especiales, como en campos de texto, APIs o aplicaciones móviles.

4. Escapar caracteres especiales utilizando la sintaxis de caracteres específica para el intérprete que se trate.
5. Utilizar LIMIT y otros controles SQL dentro de las consultas para evitar la fuga masiva de registros en caso de inyección SQL.

Procedimiento No 11: Proteger los métodos de autenticación

1. Implementar la autenticación multifactor para evitar ataques automatizados, de fuerza bruta o reúso de credenciales robadas.
2. No permitir el uso de credenciales por defecto en su software, particularmente en el caso de administradores, solicitar el cambio de contraseña en el primer inicio de sesión.
3. Implemente controles contra contraseñas débiles. Cuando el usuario ingrese una nueva clave, la misma puede verificarse contra la lista del Top 10.000 de peores contraseñas.
4. Utilizar mensajes genéricos iguales en todas las salidas para asegurar que el registro, la recuperación de credenciales y el uso de APIs no permitan ataques de enumeración de usuarios.
5. Limitar o incrementar el tiempo de respuesta de cada intento fallido de inicio de sesión. Registrar todos los fallos y avisar a los administradores cuando se detecten ataques de fuerza bruta.
6. Utilice un gestor de sesión en el servidor, integrado, seguro y que genere un nuevo ID de sesión aleatorio con alta entropía después del inicio de sesión.
7. Evitar el uso de IDs de usuarios en la URL, esta información debe almacenarse de forma segura y ser invalidado después del cierre de sesión o de un tiempo de inactividad determinado por la criticidad del negocio.

Procedimiento No 12: Prevenir la exposición de datos sensibles

1. Clasificar los datos procesados, almacenados o transmitidos por el sistema. Identificar qué información es sensible de acuerdo a las regulaciones, leyes o requisitos del negocio.
2. Aplicar los controles adecuados para la clasificación de información.
3. No almacenar datos sensibles innecesarios, los datos que no se almacenan no pueden ser robados.
4. Cifrar todos los datos sensibles cuando sean almacenados, además se deben cifrar los datos en tránsito con protocolos seguros como TLS (HTTPS).

5. Utilizar algoritmos y protocolos estándares y fuertes e implemente una gestión adecuada de claves. No cree sus propios algoritmos de cifrado.
6. Deshabilitar el almacenamiento en cache de datos sensibles.
7. Almacenar las contraseñas utilizando funciones de hashing adaptables con un factor de trabajo además de SALT, como Argon2, scrypt, bcrypt o PBKDF2.
8. Verificar la efectividad de sus configuraciones y parámetros de forma independiente.

Procedimiento No 13: Prevenir la pérdida de control de acceso

1. Aplicar el control de acceso del lado del servidor o en Server-less API, donde el atacante no puede modificar la verificación de control de acceso o los metadatos.
2. A excepción de los recursos públicos, se debe denegar de forma predeterminada el acceso a todos los recursos.
3. Implementar los mecanismos de control de acceso una vez y reutilícelo en toda la aplicación, incluyendo minimizar el control de acceso HTTP (CORS).
4. Los controles de acceso al modelo deben imponer la propiedad de los registros, en lugar de aceptar que el usuario puede crear, leer, actualizar o eliminar cualquier registro.
5. Deshabilitar el listado de directorios del servidor web y asegurar los metadatos/fuentes de archivos y copias de seguridad para que no estén presentes en las carpetas públicas.
6. Registrar errores de control de acceso y alerte a los administradores cuando corresponda.

Procedimiento No 14: Evitar configuraciones de seguridad por defecto

1. Implementar procesos de fortalecimiento reproducibles que agilicen y faciliten la implementación de otro entorno asegurado. Los entornos de desarrollo, de control de calidad (QA) y de producción deben configurarse de manera idéntica y con diferentes credenciales para cada entorno. Este proceso puede automatizarse para minimizar el esfuerzo requerido para configurar cada nuevo entorno seguro.
2. Utilizar plataformas minimalistas sin funcionalidades, componentes y documentación innecesarios. Elimine o no instale frameworks y funcionalidades no utilizadas.
3. Revisar y actualizar las configuraciones apropiadas de acuerdo a las advertencias de seguridad y siga un proceso de gestión de parches. En particular, revise los permisos de almacenamiento en la nube.

4. La aplicación debe tener una arquitectura segmentada que proporcione una separación efectiva y segura entre componentes y acceso a terceros, contenedores o grupos de seguridad en la nube (ACLs).
5. Utilizar procesos automatizados para verificar la efectividad de los ajustes y configuraciones en todos los ambientes.

Procedimiento No 15: Prevenir los ataques XSS

1. Prevenir XSS requiere mantener los datos no confiables separados del contenido activo del navegador.
2. Utilizar frameworks seguros que, por diseño, automáticamente codifican el contenido para prevenir XSS.
3. Codificar los datos de requerimientos HTTP no confiables en los campos de salida HTML resuelve los XSS Reflejado y XSS Almacenado.
4. Aplicar codificación sensitiva al contexto, cuando se modifica el documento en el navegador del cliente, ayuda a prevenir DOM XSS.
5. Habilitar una política de seguridad de contenido (CSP) es una defensa profunda para la mitigación de vulnerabilidades XSS, asumiendo que no hay otras vulnerabilidades que permitan colocar código malicioso vía inclusión de archivos locales, bibliotecas vulnerables en fuentes conocidas almacenadas en cdns (redes de distribución de contenidos) o localmente.

Procedimiento No 16: Utilizar únicamente componentes de fuentes confiables

1. Remover dependencias, funcionalidades, componentes, archivos y documentación innecesaria y no utilizada.
2. Utilizar una herramienta para mantener un inventario de versiones de componentes tanto del cliente como del servidor. Por ejemplo, Dependency Check y retire.js.
3. Monitorizar continuamente fuentes como CVE y NVD en búsqueda de vulnerabilidades en los componentes utilizados. Utilizar herramientas de análisis automatizados.
4. Suscribirse a alertas de seguridad de los componentes utilizados.
5. Utilizar componentes únicamente de orígenes oficiales utilizando canales seguros.
6. Utilizar paquetes firmados con el fin de reducir las probabilidades de uso de versiones manipuladas maliciosamente

7. Supervisar bibliotecas y componentes que no poseen mantenimiento o no liberan parches de seguridad para sus versiones obsoletas o sin soporte.
8. Cada organización debe asegurar la existencia de un plan para monitorizar, evaluar y aplicar actualizaciones o cambios de configuraciones durante el ciclo de vida de las aplicaciones.

Procedimiento No 17: Registrar las incidencias y monitorear las actividades sospechosas

1. Asegúrese de que todos los errores de inicio de sesión, de control de acceso y de validación de entradas de datos del lado del servidor se pueden registrar para identificar cuentas sospechosas. Mantenerlo durante el tiempo suficiente para permitir un eventual análisis forense.
2. Asegúrese de que las transacciones importantes cuenten con la debida auditoría con controles de integridad para prevenir alteraciones o eliminaciones.
3. Asegúrese que todas las transacciones de alto valor poseen una traza de auditoría con controles de integridad que permitan detectar su modificación o borrado, tales como una base de datos con permisos de inserción únicamente u similar.
4. Establecer una monitorización y alerta efectivos de tal manera que las actividades sospechosas sean detectadas y respondidas dentro de períodos de tiempo aceptables.
5. Establecer un plan de respuesta o recuperación de incidentes. Existen frameworks de protección de aplicaciones de código abierto tales como OWASP AppSensor, firewalls de aplicaciones web como ModSecurity utilizando el Core Rule Set de OWASP, y software de correlación de registros con paneles personalizados y alertas.

5.1.6.5 Seguridad de operaciones

Medidas generales:

- La institución deberá contar con un responsable de la Unidad de Tecnologías que se encargará de la ejecución de procedimientos en relación con la alta dirección, del mismo modo en la evaluación del cumplimiento de las políticas y lineamientos se seguridad.

- La institución deberá contar con un Especialista de Seguridad Informática designado, el cual no realiza tareas vinculadas con la administración de la red, los sistemas y los diferentes servicios.

- La introducción de nuevas tecnologías de la información en la institución será previamente analizada y autorizada por la alta dirección, el responsable de la Unidad de Tecnologías y el Especialista de Seguridad Informática.

- La asignación y actualización de credenciales de acceso corresponde a la Unidad de Tecnologías (Anexo K. Acta entrega de credenciales y roles de usuario).

- Las aplicaciones que se utilizan en la entidad son las aprobadas por el responsable de la Unidad de Tecnologías.

Procedimiento No 18: Corrección de errores y brechas de seguridad

1. Preservar las trazas de auditoría de los sistemas en los soportes habilitados al efecto por un tiempo no menor de un año.
2. Ejecutar las herramientas de seguridad autorizadas en la entidad (Anexo C. Listado de software autorizado).
3. Generar el informe de incidencias encontradas (Anexo G. Ficha técnica para el registro de incidencias).
4. En caso de detectarse nuevas vulnerabilidades, proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.

   Responsable: Responsable de la Unidad de Tecnologías y Especialista de Seguridad Informática
5. Informar al Especialista de Seguridad Informática las acciones de emergencias ejecutadas para garantizar la seguridad del sistema.

   Responsable: Administrador de red
6. Documentar en el registro de incidencias de seguridad informática las acciones ejecutadas.
7. Determinar si es necesario realizar cambios en el sistema de seguridad informática diseñado. Diseñar la nueva estrategia a seguir.
8. Realizar un control trimestral de este procedimiento e informar de sus resultados a la Dirección Administrativa y Unidad de Tecnologías

   Responsable: Comisión designada
9. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa y Unidad de Tecnologías

Procedimiento No 19: Realización de inspecciones de seguridad informática

1. Confeccionar un cronograma con fechas tentativas de inspecciones de seguridad informática de la institución.
2. Presentar el cronograma de inspecciones a la alta dirección para su aprobación.
3. Ejecutar el cronograma de inspecciones según su planificación.
4. Chequear las tareas funcionales que debe efectuar cada cual de acuerdo a su responsabilidad.
5. Realizar inspecciones independientes a cada una de las máquinas, efectuando pruebas en las que trate de violentar las medidas de seguridad.
6. Registrar los resultados en el registro de inspecciones de los equipos.
7. Aquellos hechos que comprometan la seguridad informática serán anotados en el registro de incidencias.
8. Realizar un informe técnico con los resultados de la inspección y hacerlo llegar a la Dirección Administrativa.

   Responsable: Especialista de Seguridad Informática
9. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

Procedimiento No 20: Introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones

1. Solicitar la aprobación de la Dirección Administrativa para la instalación del nuevo sistema informático, actualización o versión.

   Responsable: Responsable del área requirente
2. Aprobar o denegar solicitud.

   Responsable: Dirección Administrativa
3. Notificar al responsable de la Unidad de Tecnologías sobre la medida tomada (aprobación o negación).

   Responsable: Responsable del área requirente
4. En caso de aceptación, se comprueba que el del nuevo sistema informático, actualización o versión cumple con el sistema de seguridad establecido en la institución.

Responsable: Responsable de la Unidad de Tecnologías y Especialista de Seguridad Informática.

5. Instala y configura el nuevo sistema informático, actualización o versión (Anexo E. Hoja de vida de los equipos informáticos).

   Responsable: Unidad de Tecnologías

6. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

5.1.6.6 Identificación, autenticación y control de acceso

Medidas generales:

- Las credenciales de acceso de los usuarios serán otorgadas únicamente por la Unidad de Tecnologías, lo cual será notificado por el jefe de área correspondiente o por la Dirección de Talento Humano (Anexo K. Acta entrega de credenciales y roles de usuario).

- Estas credenciales serán eliminadas por la Unidad de Tecnologías en cuanto el personal cese de sus funciones en la institución.

Procedimiento No 21: Autentificación de usuarios

1. Cada PC contará exclusivamente con una cuenta estándar para los funcionarios a los que se les ha asignado.
2. La cuenta de administrador estará habilitada únicamente para la Unidad de Tecnologías y su administración.
3. El funcionario accederá al ordenador con el usuario que le sea asignado.

   Responsable: Unidad de Tecnologías

4. Realizar periódicamente un control de la autenticación de usuarios.

   Responsable: Especialista de Seguridad Informática

5. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

Procedimiento No 22: Cambio de contraseña de usuarios

1. Definir un tiempo mínimo de 3 meses para el cambio de contraseña de usuario, por lo que al cumplirse el plazo se notificará al iniciar la sesión que debe realizarse el cambio de la misma.

   Responsable: Unidad de Tecnologías

2. Cambiar la contraseña cuando esta expira o solicitar a la Unidad de Tecnologías el cambio de contraseñas antes del tiempo definido.

   Responsable: Funcionarios

3. En los sistemas propietarios se establecerá el vencimiento de contraseña de acuerdo a la parametrización de tiempo.

4. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

5.1.6.7 Seguridad ante programas malignos

Medidas generales:

- Cada funcionario es responsable de efectuar el chequeo de unidades extraíbles que se autoricen introducir en el ordenador antes de su utilización.

- La Unidad de Tecnologías se encargará de la correcta instalación y actualización del Software Antivirus.

- La actualización del software antivirus de las máquinas y servidores de la red se realizará diariamente, de forma programada.

- La actualización del software antivirus en los ordenadores de los funcionarios será responsabilidad de la Unidad de Tecnologías.

- Cada funcionario es responsable de comprobar la correcta actualización del software antivirus instalado en el ordenador a su cargo.

Procedimiento No 23: Actualización del software antivirus en el servidor

1. El servidor de software antivirus se actualizará periódicamente desde la base de datos del proveedor con el fin de contar con los registros al día de código malicioso (Anexo E. Hoja de vida de los equipos informáticos).

2. Chequear periódicamente si la versión instalada es la actual según el proveedor.

Responsable: Especialista de Seguridad Informática

3. Chequear periódicamente la actualización del antivirus en el servidor.

   Responsable: Especialista de Seguridad Informática

4. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

Procedimiento No 24: Actualización del software antivirus en los ordenadores conectados a la red local.

1. Los equipos conectados a la red local se actualizarán periódicamente según la parametrización establecida en el servidor antivirus.
2. En caso de estar apagados los ordenadores en el horario previsto, el antivirus se actualizará apenas se encienda el equipo.
3. Este procedimiento será registrado en el registro de cambios de los equipos (Anexo E. Hoja de vida de los equipos informáticos).
4. Chequear la correcta actualización del antivirus.

   Responsable: Usuario del equipo y Especialista de Seguridad Informática

5. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

Procedimiento No 25: Descontaminación de programas malignos

1. Al detectarse un programa maligno en el ordenador, detener la actividad que se esté efectuando e informar a la Unidad de Tecnologías.
2. Desconectar el cable de red de la PC e identificar qué tipo de virus es el que se aloja en el ordenador.
3. Verificar que el software antivirus instalado esté debidamente actualizado. En caso de no cumplirse, actualizarlo y proceder con la descontaminación del equipo. De ser exitosa la descontaminación del virus poner en marcha el equipo.
4. Revisar las unidades extraíbles que pudieron ser afectados por el virus.
5. Investigar las causas de aparición del código maligno, identificar responsables y disponer acciones correctivas
6. Dejar constancia del suceso en el registro de incidencias del ordenador (Anexo G. Ficha técnica para el registro de incidencias).

7. Si es un programa maligno desconocido, proceder al aislamiento del fichero contaminado según el procedimiento para aislar virus y remitirlo a la Unidad de Tecnologías.

   Responsable: Especialista de Seguridad Informática

8. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

5.1.6.8 Respaldo de la información

Medidas generales:

- Se realizarán copias de seguridad de la información y del software que se determine y se comprobarán con regularidad.
- Garantizar un recurso en red compartido con carpetas particulares para cada usuario, en la cual se realizan las debidas copias de seguridad de la información más importante de cada funcionario.
- Cada funcionario será responsable de la información que guarde en el recurso compartido de acuerdo a la periodicidad con que realice las salvas personales.
- Los responsables de las unidades o direcciones son los responsables de organizar los respaldos de la información del área respectiva, definiendo la información a respaldar y el funcionario encargado.
- En el caso de la información clasificada el respaldo debe ser hecha sólo por personal autorizado para el procesamiento de este tipo de información.

Procedimiento No 26: Respaldo de la información de servidores de aplicaciones y base de datos.

1. Diariamente según el esquema de copias de seguridad programado, se efectúa el respaldo de la información de cada servidor.
2. Planificación programada de respaldos de información para los servidores:
   a. Base de datos (Respaldo de información - SQL)

      Días: LMMJVSD

      Hora: 23:00

b. Aplicaciones (Respaldo de ficheros subidos por los usuarios: pdf, imágenes de perfil, certificados digitales, etc)

   Días: LMMJVSD

   Hora: 20:00

3. El respaldo se aloja de manera temporal en un equipo de respaldos local dentro de la misma red.
4. Eventualmente se genera una copia a equipos externos a las instalaciones los fines de semana.

   Responsable: Especialista de Seguridad Informática
5. Es procedimiento se documenta con una ficha de registro de copias de respaldo (Anexo L. Ficha de respaldo de información).
6. Controlar periódicamente el cumplimiento de este procedimiento.

   Responsable: Especialista de Seguridad Informática
7. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

5.1.6.9 Gestión de incidentes de seguridad

Procedimiento No 27: Divulgación de información no autorizada

1. Informar al responsable de la unidad o dirección en la que se da el evento y a la Unidad de Tecnologías (Anexo G. Ficha técnica para el registro de incidencias).

   Responsable: Persona que presencie el incidente
2. Cancelar la operación que está realizando o eliminar la copia de información realizada del lugar en que se encuentre una vez que sea posible eliminar la evidencia.
3. Chequeará los permisos y privilegios de cada usuario y de los sistemas.

   Responsable: Responsable de la unidad
4. Prevenir la posibilidad de que se repita el hecho.

   Responsable: Especialista de Seguridad Informática
5. Formar una comisión responsable para investigar los hechos.
6. Procede a aplicar las medidas disciplinarias según correspondan

Responsable: Responsable de la unidad

7. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Responsable de la unidad

Procedimiento No 28: Acceso pirata a la red

1. Informa al responsable de la unidad y al Especialista de Seguridad Informática.

   Responsable: Persona que lo detecte

2. Informa a la Unidad de Tecnologías y a la Dirección Administrativa

   Responsable: Especialista de Seguridad Informática

3. Chequear periódicamente la red en busca de vulnerabilidades

4. Si el ataque procede de la propia entidad: La Unidad de Tecnologías revisa los permisos otorgados, las bitácoras en los servidores (logs) y gestiona o realiza un diagnóstico interno para precisar fallas que pudieran ser aprovechadas por el atacante.

5. Si el ataque procede del exterior: La Unidad de Tecnologías revisa el firewall o router de salida. Determinar la existencia de vulnerabilidades en los servidores efectuando o coordinando un diagnóstico (Anexo G. Ficha técnica para el registro de incidencias).

   Responsable: Especialista de Seguridad Informática

6. Se registra el hecho en el registro de incidencias de la seguridad informática.

   Responsable: Especialista de Seguridad Informática

7. Se investigan y analizan las vulnerabilidades en el sistema de seguridad que propiciaron los hechos. De acuerdo con la trascendencia del ataque se involucra a los órganos competentes.

   Responsable: Dirección Administrativa

8. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

Procedimiento No 29: Fallo de hardware

1. Informa al responsable de la unidad o dirección y a la Unidad de Tecnologías

   Responsable: Persona que lo detecte

2. Contacta a técnicos encargados de reparación y mantenimiento del equipamiento o al proveedor quien entregó el equipamiento defectuoso

Responsable: Unidad de Tecnologías

3. Informa al Especialista de Seguridad Informática de ser una máquina contentiva de información clasificada.

   Responsable: Unidad de Tecnologías

4. Si es necesario extraer el equipo y se trata de una máquina que alberga información clasificada se debe retirar el disco del equipo. Si esto no es posible, la información que contiene debe ser extraída por el personal autorizado en otro soporte y borrada del disco antes de la salida de la institución.

   Responsable: Especialista de Seguridad Informática

5. Analizan el fallo ocurrido y ejecuta las acciones para la reparación del equipo.

   Responsable: Responsable del mantenimiento o reparación

6. Registra el evento sucedido en el historial de equipo (Anexo G. Ficha técnica para el registro de incidencias y Anexo E. Hoja de vida de los equipos informáticos).

   Responsable: Especialista de Seguridad Informática

7. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Dirección Administrativa

Procedimiento No 30: Fallo de Software

1. Apaga el equipo y alerta que no sea usado, además informa al responsable de la unidad y a la Unidad de Tecnologías.

   Responsable: Persona que lo detecte

2. Contacta a técnicos encargados de la administración de los sistemas de gestión de datos según corresponda.

   Responsable: Unidad de Tecnologías

3. Restaura versión original del software o soportes con los respaldos de los sistemas operativos o las aplicaciones.

4. Informan que los equipos y sus aplicaciones están restaurados para su uso.

   Responsable: Unidad de Tecnologías

5. Realizan anotaciones de este hecho en el registro de incidencias.

   Responsable: Especialista de Seguridad Informática

6. Chequear periódicamente el cumplimiento de este procedimiento.

   Responsable: Unidad de Tecnologías

Procedimiento No 31: Destrucción o modificación de la información

1. Informar al responsable de la unidad o dirección, además del Especialista de Seguridad Informática.

   Responsable: Responsable de la unidad o dirección que lo detecte

2. Tratar de determinar las causas o debilidades en la seguridad de los sistemas que propiciaron los hechos para corregirlas.

   Responsable: Especialista de Seguridad Informática

3. Investigar los posibles causantes para tomar las medidas disciplinarias correspondientes.

   Responsable: Responsable de la unidad

4. Procede informar al personal encargado del respaldo de la información afectada para que sea restaurada a partir de las copias realizadas previamente.

   Responsable: Responsable de la unidad

5. Registrar las novedades en el registro de incidencias.

   Responsable: Especialista de Seguridad Informática

6. Chequear periódicamente el cumplimiento de este procedimiento

   Responsable: Dirección Administrativa

5.1.7. Plan de implementación de alto nivel

Esta sección toma lugar después de haber identificado los riesgos, amenazas y vulnerabilidades, con el fin de determinar las actividades a ser implementadas por la organización, las cuales permiten ajustar el nivel de seguridad existente con las exigidas por las políticas de seguridad elaboradas en el apartado anterior.

Las actividades a ser realizadas por la institución son las siguientes:

- Clasificación de la información
- Inventario de acceso a los sistemas
- Concientización a los usuarios

- Revisión de procedimientos complementarios
- Cronograma de implementación

5.1.7.1 Clasificación de información

Clasificar la información utilizada por la organización con la finalidad de estimar los recursos a usar para brindar distintos niveles de protección a la información según sea el necesario. La clasificación de la información comprende de las siguientes etapas:

- Elaborar un inventario de activos de información incluyendo información almacenada en medios digitales extraíbles.
- Definir los custodios para los activos identificados.
- Clasificar la información por parte de los custodios.
- Consolidar los activos de información clasificados.
- Determinar las medidas de seguridad a ser aplicados para cada activo clasificado en relación a los niveles de acceso de su custodio.
- Implementar las medidas de seguridad previamente determinadas.

5.1.7.2 Inventario de acceso a los sistemas

Realizar un inventario en base a los accesos que tiene cada usuario dentro de las plataformas institucionales. Este inventario debe estar ligado al perfil de acceso de cada usuario, para el inventario se considera las siguientes etapas:

- Elaborar un inventario de los sistemas de la institución.
- Elaborar un inventario de perfiles de acceso a cada sistema.
- Analizar los perfiles de acceso en los sistemas para cada usuario.
- Revisar y aprobar el acceso por parte de los responsables de unidades o direcciones.
- Realizar un mantenimiento periódico de este inventario.

5.1.7.3 Concientización a los usuarios

Realizar una campaña de concientización para el personal que en sus actividades diarias se encuentra el uso los activos de información. Para este procedimiento se deben tomar en cuenta los siguientes procedimientos:

- Definir el mensaje a transmitir y material a ser empleado para los usuarios, entre ellos:
    - Personal en general: cultura preventiva sobre seguridad, políticas y estándares; protección contra virus, nivel de seguridad de contraseñas, seguridad física, sanciones por incumplimientos, uso inadecuado de Internet, etc.
    - Personal de tecnologías: Políticas de seguridad, estándares y controles específicos para la tecnología.
    - Direcciones: Monitoreo de seguridad, responsabilidades de supervisión, políticas de sanción. Identificar al responsable de informar los temas de seguridad en cada departamento.
- Establecer un cronograma de capacitación y realizar la campaña según el cronograma elaborado, manteniendo siempre actualizado el registro de capacitación del personal.

5.1.7.4 Revisión de procedimientos complementarios

Adoptar los procedimientos y controles complementarios de la organización de acuerdo a lo estipulado en las políticas de seguridad planteadas en el apartado anterior. Las etapas que se adoptarán en esta revisión son:

- Revisar los controles y estándares para desarrollo de sistemas.
- Elaborar procedimientos de monitoreo, verificar periódicamente carpetas compartidas, generar copias de respaldo de información de usuarios, aplicar controles de seguridad para información en equipos portátiles, etc.
- Elaborar procedimientos de monitoreo y reporte sobre la administración de los sistemas y herramientas de seguridad, entre ellas: antivirus, servidores de aplicaciones, servidores de base de datos, etc.
- Establecer controles para la transmisión de información entre clientes y proveedores.
- Establecer controles para usuarios externos que acceden a los sistemas de la institución.

5.1.7.5 Cronograma de implementación

Las actividades antes mencionadas deben ser lideradas por la Unidad de Tecnologías y sus responsables deben ser definidos individualmente para cada uno de ellos. Por lo tanto, se ha definido un cronograma tentativo dentro de los meses de noviembre de 2019 a enero de 2020. A continuación, se detalla las fechas del cronograma de implementación.

Tabla 18-5. Cronograma de implementación del plan de seguridad

Actividad	**2019-11**	**2019-12**	**2020-01**
Clasificación de información			
Inventario de acceso a los sistemas			
Concientización a los usuarios			
Revisión de procedimientos complementarios			
Revisión por la Unidad de Tecnologías			
Aprobación por la dirección			

Elaborado por: Pinango Álvaro, 2020

CONCLUSIONES

- Aplicando la metodología de pentesting se pudo analizar que la plataforma informática del Cuerpo de Bomberos del GAD Municipal de Santo Domingo, cuenta con 6 dispositivos, y al seguir la guía OWASP Top10-2017 donde se menciona los ataques más potenciales que sufren los servicios web, se llegó a la conclusión que la plataforma fue expuesta ante 8 de las 10 vulnerabilidades, entre ellas: exposición de información sensible, inseguridad en el método de inicio de sesión, envío de información confidencial sin cifrado alguno, puertos abiertos que no se encontraban en uso y fácil acceso a usuarios no autorizados.

- Mediante la explotación y análisis de vulnerabilidades realizados a la plataforma se pudo constatar que las 8 vulnerabilidades escaneadas pueden ser prevenidas, por ello, se determina las nuevas medidas, políticas y la necesidad de la implementación de procedimientos que permitan mejorar el nivel de seguridad de la información, además, de que brinden el soporte necesario para prevenir la aparición de nuevas vulnerabilidades con el paso del tiempo.

- Luego de haber llevado a cabo el proceso de elaboración del plan de seguridad basado en la norma ISO 27001, conjuntamente con las 8 vulnerabilidades más críticas identificadas en base al OWASP Top10-2017, y una vez realizada la revisión por la Unidad de Tecnologías, socialización, concientización y aprobación de dicho plan por la alta dirección, se logró mejorar el nivel de seguridad, reduciendo de 8 a 2 vulnerabilidades encontradas.

- Con la implementación del plan de seguridad se alcanza a mejorar el nivel de seguridad de la plataforma informática en un 75%, considerando que las dos vulnerabilidades no superadas, como la exposición de datos sensibles puede ser prevenida mediante la implementación de protocolos confiables de cifrado que eviten la captura de paquetes enviados por la plataforma. Del mismo modo sucede con la exposición por implementación de componentes con vulnerabilidades conocidas, se puede mantener una exposición mínima mediante el uso de componentes de fuentes confiables y la revisión constante de nuevas vulnerabilidades detectadas asociadas a los componentes utilizados en la plataforma.

RECOMENDACIONES

- Solicitar autorización a la directiva de la organización para realizar las pruebas correspondientes, de modo que la organización se encuentre al tanto de las actividades realizadas y se evite conflictos ocasionados por malos entendidos o falsas alarmas entre personal técnico y los investigadores.

- Documentar acuerdos de confidencialidad y no divulgación de la información institucional para cualquiera que sea la actividad realizada por personal interno o externo que se vea envuelta con el manejo de todo tipo de información.

- Cuando se utiliza un servidor propio y/o en producción, se recomienda contar con el acceso físico, así como de contar con privilegios de usuario, es decir, restringir el acceso solo a personal autorizado para los respectivos procedimientos.

- Para proteger la exposición de datos sensibles, se recomienda utilizar algoritmos y protocolos fuertes que cifren los datos, de esta manera si un atacante llegase a interceptar dichos paquetes no los podrá entender y no le serán de utilidad.

- En realización a las vulnerabilidades que no pudieron ser mitigadas en componentes de la plataforma, se recomienda hacer uso únicamente de componentes de fuentes confiables o canales seguros. Utilizar preferentemente paquetes firmados con el fin de reducir las probabilidades de uso de versiones manipuladas maliciosamente.

- Revisar periódicamente las actualizaciones de los sistemas informáticos, aplicaciones y herramientas de desarrollo, en vista que mediante las mismas se implementan parches de seguridad y errores encontrados en versiones anteriores.

- Se recomienda contar con un servicio de un respaldo en la nube para los servidores de aplicaciones y base de datos.

BIBLIOGRAFÍA

ACISSI. (2018). *Seguridad informática : hacking ético : conocer el ataque para una mejor defensa*. ENI.

Advisera. (2019). ¿Qué es norma ISO 27001? Retrieved January 20, 2020, from https://advisera.com/27001academy/es/que-es-iso-27001/

Aguilera Lopez, P. (2010). *Seguridad informática*. Retrieved from https://books.google.com.ec/books?hl=es&lr=&id=Mgvm3AYIT64C&oi=fnd&pg=PA1&dq=plan+de+seguridad+informática&ots=PqqkSEEIVY&sig=HbP0mQ5fxfaed5c_UARrWf4ohP4&redir_esc=y#v=onepage&q=plan de seguridad informática&f=false

Ali, Shakeel; Allen, Lee; Heriyanto, T. (2014). Kali Linux – Assuring Security by Penetration Testing. *Network Security*, *2014*(8), 4. https://doi.org/10.1016/s1353-4858(14)70077-7

Amado Ballen, J. W., Ayala Calderón, C. A., & Sierra Morales, A. A. (2017). *Análisis de vulnerabilidades en aplicaciones Web desarrolladas en PHP Versión 5.6.24 con base de datos MYSQL Versión 5.0.11 a partir de ataques SQL Inyección*. Universidad Cooperativa de Colombia, Facultad de Ingenierías, Ingeniería de Sistemas, Bucaramanga. Retrieved from http://repository.ucc.edu.co/handle/ucc/1651

Broad, J., & Bindner, A. (2013). *Hacking with Kali: Practical penetration testing techniques*. *Hacking with Kali: Practical Penetration Testing Techniques*. Elsevier Inc. https://doi.org/10.1016/C2012-0-02727-5

Castillo, J., Cisneros, A., Méndez, P., & Jácome, D. (2018). Modelo para la reducción de riesgos de seguridad informática en servicios web. *Revista Cumbres*, *4*(2), 12. Retrieved from https://dialnet.unirioja.es/servlet/articulo?codigo=6836549

Cuevas, J. C., Muñoz, R. M., Di Gionantonio, M. A., Gastañaga, I., Gibellini, F., Parisi, G., … Zea Cárdenas, M. (2018). Análisis de vulnerabilidades de sistemas web en desarrollo y en producción. Retrieved from http://sedici.unlp.edu.ar/bitstream/handle/10915/68347/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

De Jimenez, R. E. L. (2017). Pentesting on web applications using ethical - Hacking. In *2016 IEEE 36th Central American and Panama Convention, CONCAPAN 2016* (pp. 1–6).

IEEE. https://doi.org/10.1109/CONCAPAN.2016.7942364

Duque Valencia, J. (2010). *Ciberseguridad.*

Dussán Clavijo, C. A. (2006). Políticas de seguridad informática, *2*(1), 86–92. Retrieved from https://www.redalyc.org/pdf/2654/265420388008.pdf

Fox, D. (2006). Open Web Application Security Project. *Datenschutz Und Datensicherheit - DuD*, *30*(10), 636–636. https://doi.org/10.1007/s11623-006-0164-8

Gabriela Hernández Pinto, M., & Alice Naranjo Sánchez, B. (2006). DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA DEL SECTOR COMERCIAL. Retrieved January 22, 2020, from https://poseidon01.ssrn.com/delivery.php?ID=563006110027085018086081097105068110102013067092070087126002109100017095077078126113099122116002019025028002081107114018088069126032013032039092001121123029081000095057039003091064123072127016104075121109072008O

Gimeno, J. F. (2019). *Análisis, diseño y desarrollo de una aplicación para la realización automática de pentesting*.

Gómez Vieites, Á. (2019). *TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS*. Retrieved from www.keylogger.com

Guillen Zafra, J. L. (2017). *Introducción al pentesting*.

Hernández Saucedo, Ana Laura; Mejia Miranda, J. (2015). *Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web*. Retrieved from https://www.redalyc.org/pdf/5122/512251501005.pdf

ISO/IEC 27000, Nunes CQSI Ariosto Farias Junior MÓDULO Alberto Bastos MÓDULO Marcelo Gherman, F., Apresentação, Wang, L., Wijesekera, D., Jajodia, S., … Operation, S. (2018). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and. *ACM Workshop on Formal Methods in Security Engineering.Washington, DC, USA*, *34*(19), 45–55. https://doi.org/10.1016/j.im.2003.02.002

ISO 27000. (2018a). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved July 14, 2019, from http://www.iso27000.es/sgsi.html

ISO 27000. (2018b). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. Retrieved January 17, 2020, from http://www.iso27000.es/sgsi.html

ISO Tools. (2019). Implementación de controles y definición del plan de tratamiento de riesgos en un SGSI. Retrieved March 5, 2020, from https://www.isotools.org/2019/07/09/implementacion-de-controles-y-definicion-del-plan-de-tratamiento-de-riesgos-en-un-sgsi/

Lapuente, M. J. L., & Lapuente, C. L. (2013). Servicios Web. Retrieved January 17, 2020, from http://www.hipertexto.info/documentos/serv_web.htm

Muniz, J., & Lakhani, A. (2013). *Web Penetration Testing with Kali Linux*. Retrieved from https://books.google.com.ec/books?id=4fD7AAAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Nmap. (2017). Zenmap - Official cross-platform Nmap Security Scanner GUI. Retrieved December 8, 2019, from https://nmap.org/zenmap/

OWASP. (2017). OWASP Top 10, 25. Retrieved from https://github.com/OWASP/Top10/issues

OWASP. (2019). OWASP™ Foundation the free and open software security community. Retrieved November 30, 2019, from https://www.owasp.org/index.php/Main_Page

Prosultra Consultores. (2017). ¿QUE ES UNA PLATAFORMA INFORMÁTICA? Retrieved November 22, 2019, from https://sites.google.com/site/tecnopu/clients

Ramos Saky, J. M. (2006). Introducción a la seguridad. In *Aplicaciones Criptográficas Java* (pp. 21–30). Grupo Editorial Patria. Retrieved from https://books.google.es/books?hl=es&lr=&id=IhUhDgAAQBAJ&oi=fnd&pg=PP1&dq=La+seguridad+informática&ots=0WRv4DthHq&sig=Jwr1s_DQf2jZGZb5UfUusu2cKqY#v=onepage&q=La seguridad informática&f=false

Rizaldos, H. (2018). Qué es Metasploit | OpenWebinars. Retrieved March 8, 2020, from https://openwebinars.net/blog/que-es-metasploit/

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., … Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. *Introducción a la seguridad informática y el análisis de vulnerabilidades*.

https://doi.org/10.17993/ingytec.2018.46

Santo Orcero, D., & Amazon. (2017). *Pentesting con Kali : aprende a dominar la herramienta Kali para hacer tests de penetración y auditorías activas de seguridad*. Coronado. Retrieved from https://books.google.com.ec/books?id=UOQ3tAEACAAJ&dq=herramientas+analisis+de+vulnerabilidades&hl=es&sa=X&ved=0ahUKEwjQyOKWlKLlAhXhct8KHT8ZDjEQ6AEISjAF

Segovia, A. J. (2018). How to use OWASP for ISO 27001 A.14 Secure development. Retrieved March 8, 2020, from https://advisera.com/27001academy/blog/2018/04/24/how-to-use-open-web-application-security-project-owasp-for-iso-27001/

Solarte, F. N. S., Rosero, E. R. E., & Benavides, M. del C. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. *Revista Tecnológica - ESPOL* (Vol. 28). Escuela Superior Politécnica del Litoral (ESPOL). Retrieved from http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Sonu Tiwary. (2013). *Kali Linux – The BackTrack Successor*. Retrieved from http://pentestmag.com

Thongthua, A., & Ngamsuriyaroj, S. (2016). Assessment of hypervisor vulnerabilities. In *Proceedings - International Conference on Cloud Computing Research and Innovation 2016, ICCCRI 2016* (pp. 71–77). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ICCCRI.2016.19

Universidad Internacional de Valencia. (2018). Cómo crear un plan de seguridad informática fácilmente. Retrieved March 7, 2020, from https://www.universidadviu.com/crear-plan-seguridad-informatica-facilmente/

Wang, S., Gong, Y., Chen, G., Sun, Q., & Yang, F. (2013). Service vulnerability scanning based on service-oriented architecture in Web service environments. *Journal of Systems Architecture*, *59*(9), 731–739. https://doi.org/10.1016/j.sysarc.2013.01.002

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety*, *141*, 5–9. https://doi.org/10.1016/j.ress.2015.03.018

Zabala, M. E. (2017). Intrusos informáticos. Retrieved from https://es.scribd.com/document/359177179/Intrusos-informaticos-docx

ANEXOS

Anexo A. Carta de auspicio de la entidad aprobando la realización del estudio

Dirección General
CB-GADM-SD

CUERPO DE BOMBEROS
SANTO DOMINGO

Oficio N° CB-GADM-SD-DG-2019-0237-OF
Santo Domingo, 17 de octubre de 2019

Ingeniero
Álvaro Pinango
C.I. 172195318-8
Presente

De mis consideraciones

Hugo Javier Parra Chávez, con cédula de identidad N° 171102241-6 en mi calidad de Representante Legal del **CUERPO DE BOMBEROS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SANTO DOMINGO,** con RUC N° 2360003540001, AUTORIZO al Ing. Álvaro Pinango Bayas, estudiante de la IPEC-ESPOCH, realizar en nuestra institución el estudio, análisis y ejecución del proyecto de titulación de la Maestría en Seguridad Telemática.

Particular que remito a usted para su conocimiento y los fines pertinentes.

Atentamente,

CUERPO DE BOMBEROS GADM STO DGO · BOMBEROS · FUEGO · RESCATE · SANTO DOMINGO · SECRETARIA GENERAL

Ing. Hugo Parra Chávez
DIRECTOR GENERAL DEL CB-GADM-SD

ACCIÓN	NOMBRE	PUESTO	FIRMA
ELABORADO POR	VERÓNICA CANO	SECRETARIA GENERAL	

Av. Jacinto Cortez y Jorge Icaza
PBX: (02) 3959 340
info@cbsd.gob.ec

www.bomberossantodomingo.gob.ec
/CuerpoDeBomberosSantoDomingo
@BomberosSD

Anexo B. Acta entrega recepción de bienes informáticos

Dirección Administrativa
Analista de Tecnologías

CUERPO DE BOMBEROS
SANTO DOMINGO

Acta Entrega Recepción 2020-0017

En la ciudad de Santo Domingo a los 11 días del mes de febrero del 2020, comparece por una parte la Ing. Génesis Dayana Rodríguez Chávez en calidad de Analista de Tecnologías del Cuerpo de Bomberos del Gobierno Autónomo Descentralizado Municipal de Santo Domingo y la Ing. Ivan Jhesmany Rodríguez Hinojosa en calidad de Profesional en Prevención e Ingeniería del Fuego, con el objeto de dejar constancia de la entrega de los siguientes bienes.

Tabla 1: Bienes

CANTIDAD	DETALLE	MARCA	SERIE	OBSERVACIÓN
1	Teclado	Genius	UD19M2303666	Nuevo
1	Mouse	Genius	UD19M2303666	Nuevo
1	Mousepad	---	S/N	Nuevo
1	CPU	HP	MXL3472PBH	Código: 007-01-002-01984 / Usado - Buen estado
1	Disco Duro	Western Digital	WCC6Y0ET8E40	Nuevo / Disco Duro interno colocado en CPU de serial MXL3472PBH
1	Monitor 18.5'	HP	6CM3242BK3	Código: 007-01-05-1998 / Usado - Buen estado
1	UPS	Forza	171212503484	Código: 400-01-099-03515 / Usado - Buen estado

Dichos bienes servirá para desempeñar las funciones administrativas asignadas. Para constancia de la entrega firman las partes involucradas.

CUERPO DE BOMBEROS Santo Domingo ANALISTA DE TECNOLOGIAS

Ing. Génesis Rodríguez
ANALISTA DE TECNOLOGÍAS

Entregué Conforme

Ing. Jhesmany Rodríguez
PROFESIONAL EN PREVENCIÓN E INGENIERÍA DEL FUEGO

Recibí Conforme

Av. Jacinto Cortez y Jorge Icaza
PBX: (02) 3959340 EXT: 307
info@cbsd.gob.ec

www.bomberossantodomingo.gob.ec
/CuerpoDeBomberosSantoDomingo
@BomberosSD

Anexo C. Listado de software autorizado

SOFTWARE AUTORIZADO

INTRODUCCIÓN

Con la evolución de la Tecnología, cada día da paso al surgimiento de nuevas herramientas y aplicaciones que permiten la accesibilidad de nuestra información, sin embargo, dichas aplicaciones no siempre provienen de comunidades o desarrolladores de confianza, motivo por el cual la instalación de estas aplicaciones pone en riesgo la seguridad de los equipos que conforman la red y vulnera así nuestro bien más preciado, la información.

OBJETIVOS

Determinar como norma preventiva el uso exclusivo de aplicaciones y herramientas seguras y estables que sean de fuentes confiables y que no comprometa la seguridad de los equipos en los que sean instaladas.

SOFTWARE AUTORIZADO

En la tabla que se presenta a continuación se detalla el listado de software autorizado para implementación en caso de requerir el uso de cada una de las necesidades.

SISTEMA OPERATIVO	
Sistema operativo	• Para aquellos equipos que han sido adquiridos con un sistema operativo integrado se conservará su base y se permitirá la actualización del mismo: Windows 8, Windows 10, etc.
OFIMÁTICA	
Editor de documentos (Documentos, hojas de cálculos, presentaciones)	• En aquellos equipos que se han adquirido con un paquete ofimático instalado, se mantendrá el paquete y se permitirá la actualización de características. • En caso de adquirir equipos que no tengan instalado un paquete informático el software autorizado para instalar será el LibreOffice en cualquiera de sus versiones.
Editor de documentos planos (sin formato)	• Bloc de notas • WordPad • Notas rápidas (Windows)
Visor de documentos PDF	• Microsoft Edge, Google Chrome o Firefox • Nitro PDF Reader • Sumatra PDF

MULTIMEDIA	
Navegador web	• Google Chrome • Firefox • Internet Explorer • Microsoft Edge
Reproductor multimedia	• Windows media player (Windows) • Photos, Movies & Tv • VLC Player
Editor multimedia	• Paint (Windows) • Adobe Creative Suite • Editor de fotos y videos integrados
Conferencias (Chats y llamadas)	• Skype • Google Hangouts
APLICACIONES DE DESARROLLO	
Lenguajes de programación	• Java, PHP, .Net • Otras según la necesidad de las aplicaciones a desarrollar
Motores de base de datos	• SQL Server • PostgreSQL • MySQL, MariaDB • Firebase, MongoDB
Editores de código	• Notepad, Notepad++, Sublime Text • Eclipse, NetBeans, Coda, Visual Studio Code, Atom, Brackets, Vim • Microsoft Visual Studio
Virtualización de equipos	• VirtualBox • VMware
OTRAS HERRAMIENTAS	
Control remoto de equipos	• AnyDesk • TeamViewer
Visor de documentos de planos arquitectónicos	• Free DWG • Autodesk DWG Trueview • AutoCAD

FIRMAS DE RESPONSABILIDAD

Dirección General
CUERPO DE BOMBEROS DEL GAD MUNICIPAL DE SANTO DOINGO

Anexo D. Registro de entrada y salida de bienes informáticos

CUERPO DE BOMBEROS SANTO DOMINGO

FICHA DE REGISTRO
ENTRADA Y SALIDA DE BIENES INFORMÁTICOS

Estación: **Fecha:**

Responsable:

#	FUNCIONARIO	DIRECCIÓN/PUESTO	FECHA/HORA	FIRMA

Av. Jacinto Cortez y Jorge Icaza
PBX: (02) 3959340 EXT: 307
info@cbsd.gob.ec

Anexo E. Hoja de vida de los equipos informáticos

DIRECCIÓN ADMINISTRATIVA
UNIDAD DE TECNOLOGÍAS
HOJA DE VIDA DE LOS EQUIPOS

CUERPO DE BOMBEROS SANTO DOMINGO

Código de equipo:	
Fecha:	

MANTENIMIENTO CORRECTIVO Y PREVENTIVO

1. DATOS DEL EQUIPO			
Marca:		Modelo:	

2. CONFIGURACIÓN ACTUAL HARDWARE								
Placa - inventario					Marca Monitor			
Modelo CPU					Serial Monitor			
Serial CPU					Modelo Monitor			
Procesador		Velocidad			Serial Teclado			
Memoria RAM		Velocidad			Mouse		Serial	
HD marca		Capacidad		Tecnología: IDE / SCSI	Marca Impresora		Modelo Impresora	
Tarjeta de Video					Serie impresora			
Disco drive 3.5					Otros dispositivos		Serial	
CDROM								
Unidad DVD								

3. CONFIGURACION DE LA RED				
Nombre del Equipo	En red (Si/ No)	Dirección IP	Dirección MAC	Velocidad

4. SOFTWARE INSTALADO		**5. TIPO DE MANTENIMIENTOS**			
Nro.	Descripción	Versión	**Mantenimiento**		
1.			Tipo de Mantenimiento (Prev. / Corre.)		
2.			Fecha	Realizó	
3.			**Observaciones:**		
4.					
5.					
6.					
7.					
8.			**Mantenimiento**		
9.			Tipo de Mantenimiento (Prev. / Corre.)		
10.			Fecha	Realizó	
11.			**Observaciones:**		
12.					
13.					
14.					
15.					

16.			**Mantenimiento**			
17.			Tipo de Mantenimiento (Prev. / Corre.)			
18.			Fecha		Realizó	
19.			**Observaciones:**			
20.						
21.						
22.						

6. UBICACION ACTUAL					
Usuario responsable	Área/ Unidad	F. asignación	Firma	F. devolución	Firma

7. RECOMENDACIONES:_____

_____

_____

_____

_____

Anexo F. Expediente técnico de bienes informáticos

FICHA DE REGISTRO
EXPEDINTE TÉCNICO DE BIENES INFORMÁTICOS

DATOS GENERALES DEL EQUIPO			
Equipo:			
Número de serie:		**Código institucional:**	
Marca/Modelo:			
Estado del equipo:			
CUSTODIO Y DATOS DE CONFIGURACIÓN			
Nombre de custodio:		**C.C.:**	
Fecha de entrega:		**N° de acta:**	
Responsable de entrega:			
Dirección IP:			
Dirección MAC:			

REGISTRO DE EVENTOS

Evento registrado:	
Fecha de registro:	
Responsable:	
Descripción:	
F. …….. **Nombre responsable:** **Cargo responsable:**	**F. ……..** **Nombre:** **Tecnologías CB-GADM-SD**

Anexo G. Ficha técnica para el registro de incidencias

FICHA DE REGISTRO
REGISTRO DE INCIDENCIAS

DATOS DEL REGISTRO			
Estación:		**Fecha de registro:**	
Responsable de registro			
EQUIPO QUE REGISTRA EL EVENTO			
Equipo:			
Número de serie:		**Código del equipo:**	
Estado del equipo:			
Otra información:			
DESCRIPCIÓN DEL EVENTO REGISTRADO			
Fecha del evento:		**Fecha de aviso:**	
Descripción:			
DATOS DEL RESPONSABLE DIRECTO ASOCIADO CON EL EVENTO			
Nombre:			
C.C.:			
Dirección/Cargo:		**F**……	
Jefe Inmediato:			
MEDIDAS TOMADAS			
Fecha de aviso:			
¿A quién se da aviso?			
Acciones a tomar:			

RECOMENDACIONES	
1.	
2.	
3.	
4.	

F.....
Unidad de tecnologías
Cuerpo de Bomberos del GADM-SD

Anexo H. Resolución de la comisión para la baja de bienes

DIRECCIÓN ADMINISTRATIVA
UNIDAD DE TECNOLOGÍAS
FICHA DE REGISTRO – ELIMINACIÓN I.O.C.

CUERPO DE BOMBEROS
SANTO DOMINGO

Acta No. XXXX
Acta Administrativa para la baja de bienes dañados y obsoletos

En las instalaciones de Unidad de Control de Bienes (Dirección Administrativa) del Cuerpo de Bomberos del Gobierno Autónomo Descentralizado Municipal de Santo Domingo, siendo las __ horas del día __ de _____ de ____ ; el/la custodio/a _____ comparece ante la presencia del/a Analista de Control de Bienes, _____ y _____, Guardalmacén con el objeto de formalizar la baja definitiva de los bienes que se encuentran en mal estado y detallados en el **Anexo BB-XXX** al acta de validación.

Los que en la presente participan, dan fe de que se realizó el acto por el que nos encontramos reunidos, con el objeto de levantar la presente acta, para dar de baja los bienes que se detallan en el anexo antes mencionado, mismo que forma parte integral de ésta, y declara que como resultado del análisis practicado a la existencia de dichos bienes, se determina que los mismos se encuentran en condiciones inútiles a criterio de los presentes, por lo que su reparación resulta incosteable, determinándose como destino final, sean depositados en el relleno sanitario de la localidad.

Expuesto lo anterior, se da por terminada la presente diligencia, a las xxx horas del mismo día de su inicio, firmando al calce para dar constancia, quienes en ella intervinieron.

Damos fe,

F.: ……..	**F.**: ……..	**F.**: ……..
xxxxxxxxxxxxxxxxxxxx	**xxxxxxxxxxxxxxxxxxxx**	**xxxxxxxxxxxxxxxxxxxx**
Custodio/a	Analista de Control de Bienes	Guadaalmacén

Anexo BB-XXX

LISTADO DE BIENES PARA SU BAJA

Nº	CÓDIGO	F. INCIDENCIA	DESCRIPCIÓN / OBSERVACIÓN

F.: ……..
xxxxxxxxxxxxxxxxxxxx
Custodio/a

Anexo I. Expediente de eliminación de Información Oficialmente Clasificada (I.O.C)

FICHA DE REGISTRO
ELIMINACIÓN DE INFORMACIÓN OFICIALMENTE CLASIFICADA (I.O.C)

DATOS DEL REGISTRO			
Fecha de registro:		**Código de registro:**	
Responsable de registro:			
Solicitante:			
Dirección/Puesto:			
Equipo/dispositivo:			
DESCRIPCIÓN			
Última acción realizada:			
Valor de la información:			
Relación de la información:			
Motivo para eliminar:			
RESOLUCIÓN			
Fecha de comisión:		**Eliminar/Respaldar:**	
Quién preside la reunión:			
Personal relacionado:			
Respuesta:			

F……..
Unidad de tecnologías
Cuerpo de Bomberos del GADM-SD

Anexo J. Versionamiento del software

FICHA DE REGISTRO
VERSIONAMIENTO DEL SOFTWARE

DATOS DEL REGISTRO			
Fecha de registro:		**Código de registro:**	
Responsable de registro:			
Aplicación:			
SITUACIÓN ACTUAL			
Versión actual:			
Tipo de dispositivo:			
IMPLEMENTACIÓN			
Versión propuesta:		**F. inicio:**	
F. pruebas:		**F. propuesta:**	
Motivo de cambio:			
Herramientas:			
Funcionalidad:			
Pruebas realizadas:			

F……..
Unidad de tecnologías
Cuerpo de Bomberos del GADM-SD

Anexo K. Acta entrega de credenciales y roles de usuario

Dirección Administrativa
Analista de Tecnologías

CUERPO DE BOMBEROS
SANTO DOMINGO

Acta Entrega Recepción 2020-0020

En la ciudad de Santo Domingo a los 13 días del mes de febrero del 2020, comparece por una parte la Ing. Génesis Dayana Rodríguez Chávez en calidad de Analista de Tecnologías del Cuerpo de Bomberos del Gobierno Autónomo Descentralizado Municipal de Santo Domingo y el Ing. Rodríguez Hinojosa Iván Jhesmany en calidad de Profesional en Prevención e Ingeniería del Fuego del Cuerpo de Bomberos del Gobierno Autónomo Descentralizado Municipal de Santo Domingo, con el objeto de dejar en constancia la entrega de las siguientes credenciales.

Tabla 1: Correo Institucional

N°	FUNCIONARIO	CORREO	CONTRASEÑA	OBSERVACIÓN
1	Ing. Rodríguez Hinojosa Iván Jhesmany	irodriguez@cbsd.gob.ec	# de cedula	*Se recomienda realizar el cambio de la contraseña*

Dicha credencial servirá para desempeñar de mejor manera las funciones administrativas. Para constancia de la entrega, firman las partes involucradas.

CUERPO DE BOMBEROS
Santo Domingo
ANALISTA DE TECNOLOGÍAS

Ing. Génesis Rodríguez
ANALISTA DE TECNOLOGÍAS

Entregué Conforme

Ing. Ing. Iván Rodríguez
PROFESIONAL EN PREVENCIÓN E INGENIERÍA DEL FUEGO
Recibí conforme

Anexo L. Ficha de respaldo de información

FICHA DE REGISTRO
RESPALDO DE EINFORMACIÓN

DATOS DEL REGISTRO			
Estación:		**Fecha de registro:**	
Responsable de registro			
Solicitante:			
Solicitud mediante:			
EQUIPO QUE REGISTRA EL EVENTO			
Equipo:			
Tipo de dispositivo:			
Número de serie:		**Código del equipo:**	
MOTIVOS DEL RESPALDO DE INFORMACIÓN			
Código de registro:		**Unidad destino:**	
Motivo de respaldo:			
Descripción:			

F……..
Unidad de tecnologías
Cuerpo de Bomberos del GADM-SD

Anexo M. Acuerdo de confidencialidad y no divulgación de la información

Dirección Administrativa
Analista de Tecnologías

CUERPO DE BOMBEROS
SANTO DOMINGO

COMPROMISO DE CONFIDENCIALIDAD DE LOS SERVIDORES/AS DEL CUERPO DE BOMBEROS DEL GADM-SD EN CUANTO AL USO Y NO DIVULGACIÓN DE INFORMACIÓN

Yo, **RODRÍGUEZ HINOJOSA IVÁN JHESMANY** con número de cédula **1721455473**, en mi calidad de **PROFESIONAL EN PREVENCIÓN E INGENIERÍA DEL FUEGO** y en consideración de la relación que mantengo con el Cuerpo de Bomberos del CB-GADM-SD, así como del acceso que se me permite a la Información, constato que:

PRIMERA.- Soy consciente de la importancia de mis responsabilidades en cuanto a no poner en peligro la integridad, disponibilidad y confidencialidad de la información que maneja el CB-GADM-SD. En concreto he leído, entiendo y me comprometo a cumplir las normas de seguridad de los Sistemas de Información y el código de ética que corresponden a mi función.

SEGUNDA.- Me comprometo a cumplir así mismo, todas las disposiciones relativas a la política de la empresa, y a no divulgar la información que reciba a lo largo de mi estancia en la Institución, subsistiendo este deber de secreto, aun después de que finalice dicha relación, más aún si esta información es de su propiedad o pertenece a usuarios de la misma o a alguna otra Sociedad que nos proporcione el acceso a dicha información cualquiera que sea la forma de acceso a tales datos, quedando absolutamente prohibido obtener copias sin previa autorización.

TERCERA.- Entiendo que el incumplimiento de cualquiera de las obligaciones que constan en el presente documento, intencionadamente o por negligencia, podrían implicar en su caso las sanciones correspondientes por parte de la Institución y la posible reclamación por parte de la misma.

CUARTA.- Manifiesto que tengo pleno conocimiento del art. 48, art. 49 y el art 50 de la Ley de Comercio Electrónico, Firmas Electrónicas, y mensajes de datos con lo cual doy conocimiento para aceptar mensajes de datos, toda vez que se me ha informado a satisfacción, de forma clara y precisa.

QUINTA.- Para constancia de lo antes dicho, suscribo el presente documento, en mi calidad de **PROFESIONAL EN PREVENCIÓN E INGENIERÍA DEL FUEGO,** en la ciudad de Santo Domingo a los 13 días del mes de febrero del 2020.

ING. IVÁN JHESMANY RODRÍGUEZ HINOJOSA
***C.C* 1721455473**