Diseño de un esquema de *hardening* para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá

OSCAR RICARDO RODRIGUEZ MARTINEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

Diseño de un esquema de *hardening* para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá

OSCAR RICARDO RODRIGUEZ MARTINEZ

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
Ing. Hernando José Peña

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., agosto 2023

DEDICATORIA

Dedico este trabajo a mi esposa quien con su comprensión y apoyo estuvo a mi lado en todas las etapas de este proceso, por darme aliento en los momentos de dificultad y exhortarme siempre a continuar para llegar al final, también lo dedico a mis hijos quienes por su cariño y comprensión han sido siempre mi razón de ser.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, a todo su cuerpo docente y administrativo que con su continuo trabajo y dedicación nos brindan la posibilidad de adelantar nuestros estudios de una forma dinámica permitiendo que sea posible llevarlos en paralelo a otras actividades.

También deseo agradecer a mi director Ingeniero Hernando José Peña y a mis tutores quienes a lo largo del proceso académico me brindaron su experiencia y orientación sin los cuales no hubiera sido posible alcanzar este logro.

CONTENIDO

pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

AMENAZA: Es cualquier persona o incidente que pudiere generar afectaciones a un sistema informático, causando perdida, destrucción o modificación de la información.

ANTIVIRUS: Software cuyo objetivo es analizar los programas activos en memoria o archivos con el fin de detectar comportamientos anómalos o código malicioso,

***BOTNET*:** conjunto de computadores o servidores que son controlados desde una ubicación central, este centro de mando puede ejecutar instrucciones generales o detalladas sobre los equipos que están infectados, se utilizan para realizar ataques coordinados o de denegación de servicio

***FIREWALL*:** software o hardware especializado que se encarga de analizar todo el tráfico que entrada o sale de una red o servidor, aplicar filtros y políticas de acceso.

INGENIERIA SOCIAL: técnica utilizada para mediante el uso de engaños lograr obtener información personal, como contraseñas, número de tarjetas de crédito entre otros.

***KEYLOGGER*:** software que se utiliza para capturar todas las pulsaciones del teclado en determinada ventana o aplicación, estos registros se envían mediante correo electrónico o servicios FTP a un atacante externo.

SERVIDOR: dispositivo electrónico conectado a una red de datos en el cual se almacenan servicios o información que son consumidos por los diferentes clientes de la red.

SISTEMA OPERATIVO: conjunto de varios programas o aplicaciones que tienen como objetivo fundamental administrar los recursos de hardware de un equipo de cómputo, también se encargan de realizar y atender todas las operaciones de entrada o salida de datos.

***SPYWARE*:** software diseñado con el objetivo de sustraer información mediante diferentes técnicas de ataque, por lo general se instala de forma residente en la memoria del equipo afectado.

TROYANO: código malicioso utilizado por ciberdelincuentes para lograr tener acceso total a un equipo de cómputo o dispositivo móvil.

VULNERABILIDAD: es una falla o debilidad presente en los sistemas de información que esta debilidad supone un riesgo la información almacenada ya que

puede permitir que un ciberdelincuente logre afectar la confidencialidad, integridad o disponibilidad de la información.

RESUMEN

Actualmente el mundo se encuentra inmerso en un proceso de rápidos cambios y avances en temas de tecnología, estos tienen como función principal cubrir necesidades, facilitar tareas rutinarias o hacer que la información sea de carácter masivo y de acceso fácil para todas las personas. Así la información se convierte en uno de los activos más importante en cualquier compañía, no obstante, el rápido crecimiento tecnológico ha generado diferentes riesgos que pueden ser aprovechados por personas mal intencionadas. Lo anterior, ha llevado a que las instituciones requieran establecer métodos y lineamientos que permitan salvaguardarla y al tiempo mantener los tres pilares de la seguridad de la información que son integridad, confidencialidad y disponibilidad.

En este contexto cobra importancia dentro las organizaciones procesos como la hardenización cuyo propósito es el fortalecimiento del sistema informático que minimice las vulnerabilidades de seguridad de la información y aumente la protección del sistema contra posibles amenazas. Dentro de estas organizaciones se encuentra la Unidad Administrativa Especial de Servicios Públicos entidad que maneja información oficial y que dentro de su renovación de infraestructura tecnológica se ha visto vulnerable a posibles riesgos en la seguridad. Por ello el objetivo de este trabajo fue diseñar un esquema de *hardening* para los servidores web de la oficina TIC de esta entidad pública de Bogotá.

Para lograr este objetivo se establecieron planes periódicos de auditoría de seguridad los cuales brindaron un panorama del estado de aseguramiento de los distintos componentes involucrados en los sistemas de información. Estos planes de auditoria arrojaron los siguientes resultados: Levantamiento de información, enumeración de servicios y aplicaciones, identificación de herramientas a utilizar para realizar el análisis de vulnerabilidades. Para ello, se realizaron tres pruebas de esquemas de seguridad: escaneo de puertos y enumeración mediante la herramienta *Nmap,* escaneo de vulnerabilidades y escaneo de aplicaciones web. Con los resultados obtenidos de las pruebas se procedió a generar un informe del estado de seguridad de los ambientes web de producción y pruebas.

Finalmente se identificó que el aseguramiento de los servidores web debe enfocarse desde dos aspectos principales, el primero aplicar las recomendaciones de *hardening*, que tienen como objetivo evitar que personas no autorizadas logren acceso al sistema operativo y el segundo es aplicar las salvaguardas asociadas a las vulnerabilidades del sistema operativo del servidor, actividad que brindará a la Unidad Administrativa Especial de Servicios Públicos la posibilidad de mantener la información segura y libre de posibles ataques externos que podrían llegar a ser de alto impacto.

ABSTRACT

Currently the world is immersed in a process of rapid changes and advances in technology, the main function of which is to cover needs, facilitate routine tasks or make information massive and easily accessible to all. Thus, information becomes one of the most important assets in any company, however, rapid technological growth has generated different risks that can be exploited by malicious persons. The foregoing has led institutions to need to establish methods and guidelines that allow it to be safeguarded and at the same time maintain the three pillars of information security, which are integrity, confidentiality and availability.

In this context, processes such as hardenization, whose purpose is to strengthen the computer system that minimizes information security vulnerabilities and increases the protection of the system against possible threats, becomes important within organizations. Within these organizations is the Unidad Administrativa Especial de Servicios Públicos, an entity that manages official information and that within its renewal of technological infrastructure has been vulnerable to possible security risks. Therefore, the objective of this work was to design a hardening scheme for the web servers of the TIC office of this public entity in Bogotá.

To achieve this objective, periodic security audit plans were established, which provided an overview of the assurance status of the different components involved in the information systems. These audit plans yielded the following results: Gathering of information, enumeration of services and applications, identification of tools to be used to perform vulnerability analysis. For this, three tests of security schemes were carried out: port scanning and enumeration using the Nmap tool, vulnerability scanning and web application scanning. With the results obtained from the tests, a report on the security status of the production and test web environments was generated.

Finally, it was identified that the security of web servers must be focused from two main aspects, the first is to apply the hardening recommendations, which aim to prevent unauthorized persons from gaining access to the operating system and the second is to apply the safeguards associated with vulnerabilities. of the server's operating system, an activity that will provide the Special Administrative Unit of Public Services with the possibility of keeping the information safe and free from possible external attacks that could have a high impact.

INTRODUCCIÓN

Con el paso del tiempo se ha evidenciado que los avances tecnológicos van íntimamente ligados a nuevos comportamientos o tácticas delictivas las cuales pueden afectar a cualquier persona u organización que haga uso de estos. Día a día aparecen nuevas debilidades en los sistemas de información o sistemas operativos, este continuo cambio ha obligado a las organizaciones a estar en un proceso de aseguramiento continuo que les brinde la seguridad de estar preparados para evitar algún tipo de ataque o en su defecto minimizar el impacto sobre las operaciones del negocio en caso de que este sea efectivo[1].

Dentro de las organizaciones que ha tenido que estar a la vanguardia de los avances tecnológicos, se encuentra la Unidad Administrativa Especial de Servicios Públicos entidad que maneja información oficial sobre temas de recolección de basuras en la ciudad de Bogotá y que dentro de su renovación de infraestructura tecnológica se ha visto vulnerable a posibles riesgos o nuevas amenazas.

Basado en lo anterior el presente proyecto tiene como objetivo identificar las posibles vulnerabilidades presentes en los cuatro servidores web, puesto que estas pueden dar pie a que la información emitida a la ciudadanía se vea comprometida generando desinformación. Para lograr este objetivo se requiere establecer planes periódicos de auditoría de seguridad los cuales brinden un panorama claro del estado de aseguramiento de los distintos componentes involucrados en los sistemas de información, esta documentación debe servir de línea base para que las organizaciones puedan llevar un registro de la evolución que en aspectos de seguridad ha tenido[2], dado que las amenazas son cambiantes con el paso del tiempo, así como el actuar de quienes tratan de explotarlas, es por este motivo que el realizar pruebas de vulnerabilidad se convierte en un requisito para toda organización que valore la importancia de su información.

Por ello el objetivo de este trabajo fue diseñar un esquema de *hardening* para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá. Hardenización o endurecimiento informático, es el proceso de minimizar las vulnerabilidades en el sistema. Esto se puede lograr, a partir de la preparación de la organización a posibles ataques informáticos con la

---

[1] WEST, Darrell M. Avance tecnológico: riesgos y desafíos. En: Openmind BBVA. [Consultado: 14 de febrero de 2023]. Disponible en: https://www.bbvaopenmind.com/articulos/avance-tecnologico-riesgos-y-desafios/

[2] COORDINACIÓN TIC. La tecnología y su impacto en la auditoría interna de las organizaciones [blog]. INCP. Colombia. 16 agosto de 2019. [Consultado: 8 de marzo de 2023]. Disponible en: https://incp.org.co/la-tecnologia-impacto-la-auditoria-interna-las-organizaciones/

implementación de medidas de seguridad resultado del levantamiento de la información, la identificación de las vulnerabilidades y la estructuración de un informe final que permita evaluar los puntos críticos y las medidas de fortalecimiento de la seguridad. De igual manera, las auditorias de seguridad deben estar alineadas con los avances tecnológicos dado que las amenazas son cambiantes con el paso del tiempo, así como el actuar de quienes tratan de explotarlas, es por este motivo que el realizar pruebas de vulnerabilidad se convierte en un requisito para toda organización que valore la importancia de su información.

1. DEFINICIÓN DEL PROBLEMA

La Unidad Administrativa Especial de Servicios Públicos maneja información oficial sobre temas de recolección de basuras en la ciudad de Bogotá, para este fin la entidad ha venido adelantando procesos de renovación tecnológica que la lleven a estar a la vanguardia en cuanto a la disponibilidad de sus servicios, esta evolución en temas de infraestructura tecnológica da pie a posibles riesgos o nuevas amenazas.

Es importante destacar que las vulnerabilidades se pueden presentar en dos ámbitos: mediante acceso físico a los servidores o mediante acceso informático, siendo este el más importante ya que es el más difícil de controlar.

Por otro lado, la institución presenta una alta rotación de personal, en el año 2021 el 70% del talento humano de la oficina TIC se vinculó en los últimos 6 meses, lo que conlleva a que el estado de seguridad de los servidores no sea conocido al detalle generando un alto riesgo sobre la información contenida en ellos.

Aunado a lo expresado anteriormente la oficina de TI de la entidad no cuenta con una documentación clara de sus procesos de aseguramiento, esta falencia de por si está generando una problemática puesto que no existe información sobre el estado inicial de la infraestructura tecnológica, así como de los cambios a que esta se ha visto sometida con el paso del tiempo, todo esto conlleva a que el encargado de la administración de la infraestructura se vea enfrentado a un panorama desconocido en cuanto a los niveles de aseguramiento de los servidores.

Basado en lo anterior el presente proyecto pretende identificar las posibles vulnerabilidades presentes en los cuatro servidores web, puesto que estas pueden dar pie a que la información emitida a la ciudadanía se vea comprometida generando desinformación.

1.1 ANTECEDENTES DEL PROBLEMA

En el área de TI de la Unidad Administrativa Especial de Servicios Públicos no se encuentran antecedentes sobre proyectos de detección de vulnerabilidades, de igual forma no se han presentado incidentes de seguridad informática que involucren los servidores web de la entidad.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo un análisis de vulnerabilidades sobre los servidores web en ambientes de pruebas y producción de la unidad Administrativa Especial de Servicios Públicos, logrará que la entidad mejore sus niveles de aseguramiento de la información a partir de procesos de *hardening* ajustado a las necesidades de su infraestructura?

2 JUSTIFICACIÓN

Con el proyecto se pretende fortalecer la seguridad de la información contenida en lo servidores web con el fin de garantizar a la ciudadanía de Bogotá que la información entregada por la institución con respecto a temas de recolección de basura, tarifas de aseo y directrices de reciclaje, es emitida de forma confiable evitando así problemas sociales que se pudieren generar por causa de información falsa o modificada respecto a temas de recolección de residuos

En el ámbito académico la pertinencia del proyecto se fundamenta en la posibilidad de fortalecer los conocimientos adquiridos llevándolos a la práctica, desarrollando de esta forma mejores competencias respecto a los diferentes escenarios que se pueden presentar en ambientes reales y generando conocimiento sobre las diferentes técnicas utilizadas para mitigar o evitar las vulnerabilidades de los sistemas informáticos.

Los procesos de análisis de vulnerabilidades permitirán identificar las diferentes amenazas a las que se enfrenta actualmente o en el futuro la organización, para así, establecer mecanismos de endurecimiento de todos los activos de información de la organización.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un esquema de *hardening* para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá a partir de un análisis de vulnerabilidades que mejore los niveles de seguridad.

3.2 OBJETIVOS ESPECÍFICOS

- Evaluar herramientas para el análisis de vulnerabilidades en servidores web mediante un análisis comparativo para su aplicación en la infraestructura tecnológica.

- Probar herramientas para la auditoria de servidores web mediante ejercicios de *pentesting* para la identificación de vulnerabilidades.

- Analizar los resultados de las pruebas de seguridad aplicadas a los servidores web mediante una revisión de los informes técnicos para el establecimiento de salvaguardas necesarias.

- Proponer estrategias de *hardening* para la infraestructura de servidores basado en marcos de buenas prácticas que permita mejorar la seguridad digital.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

En todas las organizaciones se debe tener el conocimiento de la importancia de la información y que esta debe ser almacenada de forma segura de tal manera que se minimice al máximo las posibles amenazas contra los datos que se consideren confidenciales, así como los equipos de cómputo (servidores) que la contienen, teniendo en cuenta esto es necesario definir las distintitas herramientas y conceptos que serán utilizados en el desarrollo del proyecto.

4.1.1 Elementos vulnerables de un sistema informático:

Todos los sistemas informáticos actuales se componen de cuatro elementos: software, hardware, personal humano y datos, estos sistemas están diseñados para permitir las operaciones de almacenamiento, procesamiento y transmisión de información, las operaciones de almacenamiento y transmisión son el punto clave para garantizar que los datos no sean vulnerados.

Basado en lo expuesto anteriormente los ataques a sistemas informáticos se pueden unificar en los siguientes grupos:

Intercepción: según lo expuesto por García[3] , se presenta cuando una persona no autorizada logra acceso a un recurso, los atacantes utilizan herramientas como *keyloggers* para obtener credenciales y logar acceso.

Modificación: como lo expresa Pico[4], es un ataque en contra de la integridad de la información se presenta cuando un atacante además de conseguir acceso a un recurso es capaz de modificarlo o manipularlo, como ejemplo de este ataque podemos nombrar la modificación de datos o la manipulación de un sistema para que este trabaje de manera distinta a como fue concebido, este tipo de ataques se efectúa por lo general mediante virus informáticos o troyanos.

Generación: este es un ataque contra la autenticidad de la información consiste en insertar datos u objetos modificados en el sistema informático, por ejemplo, la inyección de código a un sitio web, o inyección de registros a una base de datos este ataque a su vez se divide en ataques pasivos y ataques activos.

Interrupción: Consiste en evitar que la información logre llegar a su destino, se realiza mediante la denegación de servicios o tratando de dejar el sistema

[3] GARCIA, Noelia. Clasificación y tipos de ataques contra sistemas de información [en línea]. vLex. [Consultado: 7 de febrero de 2023]. Disponible en: https://vlex.es/vid/clasificacion-tipos-ataques-sistemas-102081

[4] PICO, Pablo. Tipos de ataque informático [blog]. El blog del ingeniero de sistemas. Colombia. [Consultado: 14 de abril de 2023]. Disponible en: https://ingenierodesistemas.co/informatica/tipos-ataques-informatico/

informático fura de funcionamiento, este es el ataque más fácil de detectar de los cuatro.

4.1.2 Seguridad de la información

Como lo expresa Isotools Excellence[5] la seguridad de la información es el conjunto de técnicas y medidas que se utilizan para salvaguardar y controlar toda la información que se encuentra dentro de una organización también se encarga de evitar que esta salga del sistema establecido en la organización, ya que los datos que manejan las organizaciones son fundamentales para el desarrollo de sus objetivos la seguridad de la información es una pieza clave en este cometido.

Cualquier organización sin importar su tamaño tiene información confidencial que puede ser de sus clientes o de sus mismos empleados y es por esto por lo que se debe establecer las medidas de seguridad necesarias para protegerlos y darles un correcto tratamiento.

La norma ISO 27001[6] establece los objetivos de la seguridad de la información y establece un modelo para la implementación de un sistema de gestión de seguridad de la información cuyo fin principal es proteger todos los activos de información como pueden ser equipos informáticos, usuarios etc.

Existen tres pilares fundamentales que se deben tener en cuenta:

- Integridad: Velázquez y colaboradores[7] definen que la integridad de la información se refiere al hecho de que la información debe ser confiable y sin modificaciones por parte de personas no autorizadas, el objetivo es garantizar la transmisión de datos en entornos seguros.
- Confidencialidad: la confidencialidad de la información es una propiedad por medio de la cual se garantiza que el acceso a esta se realice únicamente por las personas que estén autorizadas para conocerla.
- Disponibilidad: la disponibilidad de la información se refiere a que los datos deben estar disponibles para quien los necesite que pueden ser aplicaciones, personas entre otros.

---

[5] ISOTOOLS EXCELLENCE. ¿Qué es la seguridad de la información y cuantos tipos hay? [blog]. PMG SSI. 11 de marzo de 2021. [Consultado: 23 de abril de 2023]. Disponible en: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

[6] INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN - ICONTEC. Sistemas de gestión de la seguridad de la Información: Técnicas de seguridad y requisitos. NTC-ISO/IEC 27001 [en línea]. Bogotá D.C.: El Instituto, 2013. 45 p. [Consultado: 30 de noviembre de 2022]. Disponible en: https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf

[7] VELÁZQUEZ, M. Cornejo, et al. Principios de Seguridad Informática en Sistemas de Información. XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan, 2015, vol. 3, no 6. [Consultado: 12 de diciembre de 2022]. Disponible en: https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n6/e5.html

4.1.3 Seguridad informática

Se puede definir como el proceso de detectar y prevenir la utilización no autorizada de un sistema informático, el Equipo De Expertos De Ciencia Y Tecnología De La Universidad Internacional De Valencia[8] expone que implica proteger contra intrusos el uso malintencionado de los sistemas informáticos, también se trata de prevenir los accesos accidentales a estos sistemas, es necesario diferenciarla del término seguridad de la información puesto que la seguridad informática abarca una serie de medidas específicas como manejo de programas antimalware, firewalls, activación de cuentas de usuario entre otras.

En la actualidad la importancia de la seguridad informática radica en que el uso malicioso de sistemas de información de carácter privado o de los recursos internos de una empresa, pueden acarrear graves consecuencias en las áreas de la organización creando problemas financieros como productivos[9].

4.1.4 Auditoria Informática

Son un conjunto de métodos destinados a recoger y evaluar evidencia que permitan determinar si un sistema de información se encuentra en capacidad de mantener los tres pilares de la información, así como cumplir con los objetivos estratégicos de la organización haciendo un uso adecuado de los recursos tecnológicos.

4.2 MARCO CONCEPTUAL

4.2.1 Servidor

Según EKCIT[10], un servidor es un dispositivo electrónico que tiene como función principal almacenar, y distribuir información, estos utilizan un modelo de trabajo "cliente-servidor", cualquier dispositivo o aplicación que consuma o requiera información alojada en el servidor se denomina cliente y el servidor entregará la información basada en políticas de autorización previamente definidas.

Existen dos clases principales de servidores los físicos y los virtuales, los primeros

---

[8] EQUIPO DE EXPERTOS DE CIENCIA Y TECNOLOGÍA DE LA UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? [sitio web]. Universidad Internacional de Valencia. 9 de septiembre de 2016. [Consultado: 11 de diciembre de 2022]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

[9] HACKNOID. Importancia de la seguridad informática de las empresas [blog]. Uruguay. 2 de julio de 2019. [Consultado: 18 de enero de 2023]. Disponible en: https://www.hacknoid.com/hacknoid/importancia-de-la-seguridad-informatica-de-las-empresas/

[10] EUROPEAN KNOWLEDGE CENTER FOR INFORMATION TECHNOLOGY – EKCIT. Servidores [blog]. TIC Portal. 8 de julio de 2019. [Consultado: 1 de febrero de 2023]. Disponible en: https://www.ticportal.es/glosario-tic/servidores

son maquinas físicas o de hardware, generalmente en formato tipo Rack o torre también se los conoce como Host, los segundos son servidores que carecen de hardware y son implementados en base a software, los dos tipos cumplen la misma función y su única diferencia radica en su implementación

Dependiendo del rol que estos realicen dentro de una red de datos podemos encontrar varios tipos de servidores como: servidores web servidores DNS, Servidores DHCP, Servidores de Base de datos Etc.

4.2.2 *Hardening*

Se define como el endurecimiento de los sistemas con el objetivo de reducir los peligros o amenazas que puedan afectarlos, este objetivo se logra conseguir mediante el establecimiento de políticas de seguridad que preparen a los sistemas para futuros ataques informáticos.

Como lo expresa Openit[11] la premisa que un servidor que cumple una función única es más seguro que uno que cumple con varias, por esta razón, es fundamental que se elimine todo software que no sea necesario para las funciones asignadas al servidor, de igual forma se debe desactivar todos los puertos de comunicaciones que no sean necesarios para la función específica que desempeña el servidor, otras políticas que se deben seguir para lograr un *hardening* robusto pueden ser:

- Activación de sistemas de auditoría sobre las cuentas de usuario con privilegios elevados
- Establecer políticas de copia de seguridad
- Implementar un plan de recuperación de respaldos con el fin de asegurar la integridad y disponibilidad de la información contenida en estos.
- Activación y configuración de *Firewalls*
- Instalación de parches de seguridad en los sistemas operativos

Es de suma importancia tener mucho cuidado en que la aplicación de las políticas de *Hardening* no afecten el desempeño normal del servidor o la funciones que este cumple dentro de la organización.

4.2.3 Ataque Informático

Según Ecured[12] un ataque informático es una acción intencionada y organizada ejecutada por una o más personas con la intención de causar daños o problemas de funcionamiento sobre un servidor o un sistema informático.

---

[11] OPENIT. ¿Qué es el hardening de sistemas operativos? [blog]. Argentina. [Consultado: 13 de marzo de 2023]. Disponible en: https://www.openit.com.ar/que-es-el-hardening-de-sistemas-operativos/

[12] ECURED. Ataques Informáticos [blog]. 18 de julio de 2019. [Consultado: 7 de marzo de 2023]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

Estos ataques buscan hacer uso de alguna vulnerabilidad o falla presente en el software, en el *hardware* o en las personas que forman parte de la red de datos con el fin de obtener algún tipo de beneficio que generalmente es de tipo económico, las consecuencias de estos ataques pueden llegar a ser desde muy leves como una simple afectación al rendimiento de una aplicación hasta desastrosos como la indisponibilidad total de un sistema informático, cualquiera que sea la afectación del ataque logrará tener un impacto sobre la operación del servicio de la organización.

4.2.4 Vulnerabilidades Informáticas

Según lo expone Incibe[13], una vulnerabilidad es una falla o debilidad en un sistema informático que puede poner en riesgo la seguridad de la información permitiendo que un ciberdelincuente comprometa su disponibilidad, integridad y confidencialidad, es por esta razón que es necesario detectarlas y eliminarlas o mitigarlas en el menor tiempo posible. Por lo anterior las vulnerabilidades son características o condiciones propias de un activo de información que lo hace proclive a ser víctima de un ataque, ya que en la actualidad si existe una vulnerabilidad también existe una persona que intentará sacar provecho de ella.

4.2.5 Hacking Ético

Se define el hacking Ético como las acciones que una persona conocida como Hacker realiza haciendo uso de sus conocimientos avanzados en informática y seguridad para lograr encontrar fallas o debilidades en los esquemas de seguridad de un sistema, su objetivo es enumerarlas y posteriormente reportarlas a la organización de tal forma que esta adopte las medidas necesarias orientadas a corregirlas y de esta manera logar minimizar el riesgo de robo o afectación a la información.

Las personas que realizan labores de hacking Ético realizan una serie de pruebas que se conocen con el nombre de "*Pen Test*" con el objetivo de identificar fallas o debilidades para establecer planes de mitigación, también se enfoca en probar la efectividad de los diferentes esquemas de seguridad establecidos en la organización.

4.2.6 Puerto de Comunicación

Según lo expuesto por Seguidores Online[14], un puerto de comunicación tiene la función de establecer comunicación entre un equipo de cómputo y otro dispositivo que se encuentra separado de este, los puertos de comunicación más conocidos

---

[13] INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [blog]. Instituto de Ciberseguridad. España. 20 de marzo 2017. [Consultado: 12 de enero de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

[14] SEGUIDORES ONLINE. Los Puertos de Comunicación y Sus Funciones [sitio web]. [Consultado: 3 de enero de 2023]. Disponible en: https://intelectouniversal.com/comunicaciones/puertos-de-comunicacion/

son los de hardware ya que son los que podemos identificar de forma física en un equipo de cómputo, sin embargo, a nivel lógico existen otros puertos de comunicación que son intangibles y son los que utilizan las aplicaciones o el software para intercomunicarse.

Los puertos de comunicación físicos son diversos y no existe una arquitectura única para ellos ya que se han diseñado en función de la interface o dispositivo que se desea interconectar de esta forma podemos encontrar puertos de interface serial, paralela, vga, hdmi entre otras, lo que conlleva a que en algunos equipos compactos no sea posible tener una gran variedad de puertos disponibles, como solución a este problema se desarrolló el puerto USB "*Universal Serial Bus*" que tiene como objetivo estandarizar todas las interfaces de conexión en un único puerto y protocolo de comunicaciones, este puerto en la actualidad es altamente utilizado y ha evolucionado con respecto a la velocidad de trasmisión de datos, actualmente se encuentra en su versión 3.0, este puerto a pesar de ser universal necesita de una interconexión física lo que limita la movilidad de los dispositivos, con el fin de dar solución a este inconveniente se desarrollaron los puertos de conexión inalámbrica de los cuales el más representativo y utilizado actualmente es el "*bluetooth*".

Respecto a los puertos de software o también conocidos como puertos de red, Sensagent[15] plantea que es una interfaz que utiliza un software para lograr comunicarse a través de una red de datos, el modelo OSI se encarga de administrar estos puertos y en su capa 4 establece los encabezados de transporte para logar de esta forma el envío de paquetes y su posterior reensamblaje haciendo uso de un numero de puerto especifico, de esta forma una maquina podrá establecer muchas conexiones de datos en diferentes puertos utilizando únicamente una dirección IP.

Los números de puertos se identifican mediante 2 Bytes de tal forma que tenemos disponibles 65535 puertos para establecer comunicación entre aplicaciones.

En todo sistema informático existen puertos denominados como conocidos ya que se han convertido en un estándar para determinado servicio, por ejemplo, puerto 80 para servicios web HTTP, puerto 443 para servicios web HTTPS, puerto 21 para servicios FTP entre otros.

4.2.7 *Nmap*

De acuerdo con el sitio oficial *Nmap*[16] , "*Network Mapper*" es una herramienta de código abierto para realizar descubrimiento de redes y auditorias de seguridad, también se utiliza para realizar inventarios de red, esta herramienta utiliza paquetes de datos IP que no son procesados para lograr identificar que host se encuentran

[15] SENSAGENT - DICCIONARIO. Puerto de red En: diccionario.sensagent.com/ [Consultado: 14 de enero de 2023]. Disponible en: http://diccionario.sensagent.com/puerto%20de%20red/es-es/

[16] NMAP.ORG. [sitio web]. [Consultado: 13 de febrero de 2023]. Disponible en: https://nmap.org/

disponibles en una red, identificar los puertos de red que se encuentran abiertos y la aplicación que está a la escucha en ellos.

También logra realizar una enumeración de estos hosts identificando el tipo de servidor físico o virtual, sistema operativo instalado y su versión, es una herramienta bastante útil para realizar una identificación del estado inicial de una red[17] .

4.2.8 NIST

Según Acosta[18], NIST es un marco de trabajo o *framework* que se orienta en lograr reducir los riesgos que pudieren afectar la seguridad de la información de una empresa u organización se destaca por ser un marco muy simple y flexible por lo que es ideal para ser aplicado a cualquier tipo de organización

La estructura de este marco de trabajo se basa en tres partes fundamentales

- Núcleo que se orienta específicamente a realizar un conjunto de actividades encaminadas en cumplir con los objetivos de la seguridad informática
- Niveles de implementación del marco de trabajo: con el objetivo de brindar un panorama claro de los riesgos y como son estos tratados por la organización
- Perfil del Marco: alinea los requisitos de tolerancia de riesgos con los objetivos estratégicos de la organización.

4.2.9 SNMP (*Simple Network Management Protocol*)

Según Millán Tejedor[19] el protocolo SNMP es un protocolo que trabaja en la capa de aplicación con el fin de facilitar la información de gestión entre los distintos dispositivos que conforman una red, con el paso del tiempo este protocolo se ha convertido en un estándar en las redes empresariales, este protocolo brinda la posibilidad a los administradores de gestionar el rendimiento, encontrar y resolver problemas en la red.

Básicamente el protocolo SNMP tiene dos componentes básicos como lo expone

---

[17] OTEGUI GARCÍA, Alejandro. Herramientas de análisis de vulnerabilidades [Webinar]. 20 de octubre de 2017. [Consultado: 27 de enero de 2023]. Disponible en: https://es.slideshare.net/alejandro_otegui96/herramientas-de-anlisis-de-vulnerabilidades-81021908

[18]ACOSTA, David E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST [blog]. David E. Acosta Blog personal. Barcelona, España. 11 de junio de 2017. [Consultado: 20 de febrero de 2023]. Disponible en: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/

[19] MILLAN TEJEDOR, Ramón Jesús. Que es SNMP V3 (Simple Network Management Protocol versión 3) [en línea]. Consultoría estratégica en tecnologías de la información y comunicaciones. [Consultado: 1 de febrero de 2023]. Disponible en: https://www.ramonmillan.com/tutoriales/snmpv3.php

ORACLE[20], para que el protocolo funcione correctamente se necesitan estos componentes:

Una estación de gestión de redes que es donde se aloja el software de gestión que tiene como finalidad gestionar y supervisar los nodos

Nodos gestionados son dispositivos como un *router, switche* o servidor donde se encuentran los agentes de gestión de SNMP, son los encargados de realizar las solicitudes que se originan en las estaciones de gestión.

[20] ORACLE. Referencia de gestión de protocolos para SNMP e IPMI de Oracle® ILOM, versión de firmware 3.2.x. Componentes de SNMP [sitio web]. [Consultado: 10 de marzo de 2023]. Disponible en: https://docs.oracle.com/cd/E40701_01/html/E40347/z4002eb91391913.html

5 DISEÑO METODOLÓGICO

El proyecto análisis de vulnerabilidades sobre los ambientes de producción y pruebas de la Unidad Administrativa Especial de Servicios Públicos en la modalidad de proyecto aplicado busca aplicar los conocimientos adquiridos en cuanto a seguridad informática para lograr un aseguramiento óptimo de los servicios e información alojados en esta infraestructura tecnológica. Para lo que se ha establecido la siguiente metodología:

Método de Investigación: en el presente proyecto se utilizara un método de investigación deductivo el cual inicia desde lo general hacia lo particular para lograr un entendimiento general de los componentes de la infraestructura tecnológica de la organización y de esta manera poder proceder a realizar una búsqueda de debilidades o fallas que representen un riesgo para la información con esta información será posible plantear un plan de trabajo encaminado a endurecer las políticas de seguridad y de esta manera minimizar el riesgo de robo o daño a los datos sensibles de la entidad.

Para dar cumplimiento a los objetivos del proyecto se realizarán las siguientes actividades:

Levantamiento de información: Terraetica[21] expresa que la forma en la que se levanta la información puede potenciar o retrasar la metodología utilizada para el desarrollo de un proyecto

Por lo anterior expuesto se realizará un inventario detallado de todos los componentes físicos y lógicos que hacen parte de los ambientes web de producción y pruebas con el fin de conocer su estado inicial, este será el insumo principal para conocer de primera mano que tipo de servidores existen, cuál es su capacidad, estado de sistema operativo entre otros datos de relevancia.

Con este inventario inicial se creará una matriz de componentes que nos brinde un mapa claro de cada uno de los servidores y sus componentes para lograr establecer si existen riesgos de obsolescencia tecnológica en cuanto a hardware o software

Enumeración de servicios y aplicaciones una vez identificada la infraestructura fisca es necesario realizar un inventario detallado de los distintos sistemas de información o aplicaciones en los ambientes web de producción y pruebas, es fundamental asociar este inventario de aplicaciones con el inventario de hardware obtenido en el proceso de levantamiento de información a fin de determinar si existe la posibilidad que un solo servidor este alojando más de una aplicación.

[21] TERRAETICA. Levantamiento de información cualitativa y cuantitativa [sitio web]. Cátedra de Medición de impacto 2020-21. México. [Consultado: 29 de enero de 2023]. Disponible en: https://terraetica.com/levantamiento-de-informacion-cualitativa-y-cuantitativa

Es de suma importancia que en este inventario de aplicaciones se obtengan datos detallados sobre el tipo de aplicación (cliente servidor, web, etc.), *framework* utilizado (PHP, .net, etc), puertos utilizados, tipo de autenticación, protocolos de comunicación entre otros de tal forma que este sea el insumo principal para poder realizar pruebas de intrusión o vulnerabilidades de forma objetiva y precisa

En este proceso de enumeración es importante tener claro el concepto de aplicación y servicio ya que no siempre una aplicación corresponde a un servicio específico al contrario por lo general un servicio está compuesto de una o más aplicaciones[22].

Identificación de herramientas a utilizar con la información recolectada y con un conocimiento claro de los servidores que hacen parte de los ambientes de pruebas y producción se procederá a identificar las herramientas adecuadas para realizar el análisis de vulnerabilidades, para este fin se tomara como base la suite KALI LINUX, la cual contienen un compilado de numerosas herramientas de detección y análisis.

Análisis de vulnerabilidades con la información detallada y organizada los ambientes web de pruebas y producción de la entidad se procederá a realizar un análisis de vulnerabilidades para lograr identificar las debilidades o fallas presentes.

De acuerdo con lo expuesto por Wagner[23], para este fin se realizarán tres pruebas enfocadas cada una en un aspecto diferente de los esquemas de seguridad:

- Escaneo de puertos y enumeración mediante la herramienta *Nmap* se realizará una exploración inicial de los servidores con el fin de identificar que puertos se encuentran abiertos y que aplicaciones están recibiendo información por estos.

- Escaneo de vulnerabilidades: se realizará un escaneo de vulnerabilidades sobre los sistemas operativos haciendo uso de herramientas *open source* como *GreenBone* para identificar las debilidades presentes.

- Escaneo de aplicaciones web: mediante el uso de la herramienta *open source* OWASP se realizará un escaneo sobre las aplicaciones web identificadas para establecer fallas o debilidades y plantear las acciones necesarias para su mitigación

[22] CASTRO, Jandro. UN CATÁLOGO DE SERVICIOS NO ES UNA LISTA DE APLICACIONES [blog]. Proactivanet. 28 de enero de 2014. [Consultado: 30 de noviembre de 2023]. Disponible en: https://www.proactivanet.com/blog/catalogo-de-servicios/un-catalogo-de-servicios-no-es-una-lista-de-aplicaciones/

[23] WAGNER, Jarvis. ¿Cómo hacer análisis de vulnerabilidades informáticas? [en línea]. 2 de marzo de 2016. [Consultado: 3 de abril de 2023]. Disponible en: https://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

Con los resultados obtenidos de las pruebas relacionadas anteriormente se procederá a generar un informe inicial del estado de seguridad de los ambientes web de producción y pruebas el cual será entregado a el jefe de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos para su análisis respectivo.

Informe Final con base en el resultado de las pruebas realizadas se realizará un informe detallado de las vulnerabilidades y debilidades encontradas, así como de las acciones de mejora que se pueden implementar con el fin de minimizar las debilidades encontradas de tal manera que sea este informe un insumo importante para el diseño de políticas de *hardening* por parte del personal encargado de seguridad informática en la Unidad Administrativa Especial de Servicios Públicos.

6 DESARROLLO DE LOS OBJETIVOS

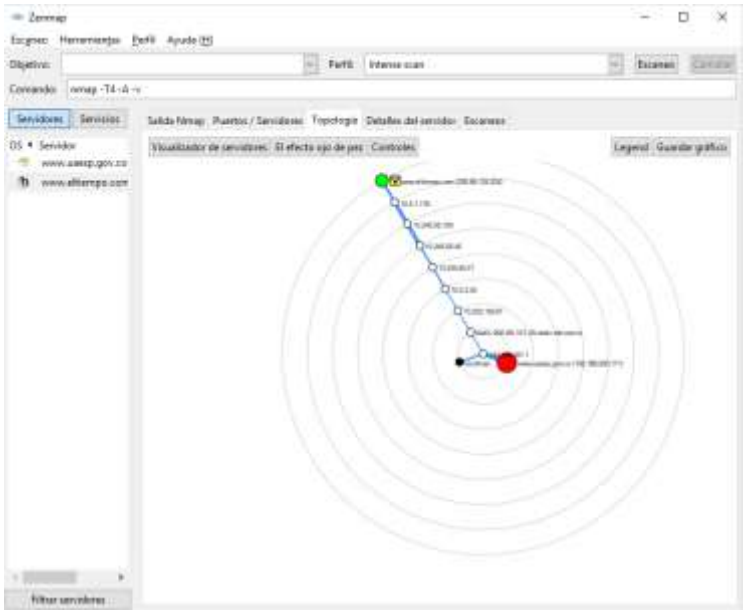
6.1 HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS DE VULNERABILIDADES

Con el fin de identificar las fallas o debilidades de una red de datos o sistema informático es necesario apoyarse en herramientas especializadas que permitan generar un panorama claro del estado actual de los elementos identificando cada una de las vulnerabilidades presentes, su impacto y la manera de minimizarlo, para este objetivo en el presente proyecto utilizaremos las siguientes:

6.1.1 NMAP (*Network Mapper*)

Es una herramienta código abierto utilizada para el descubrimiento de redes y auditoria de seguridad, Nmap utiliza paquetes IP de varias formas para lograr determinar que host están activos en la red, que servicios están ofreciendo, versión de sistema operativo y muchas otras características, esta herramienta está disponible para plataformas Linux, Mac OS X y Windows. Es fácil de utilizar para usuarios no experimentados y a su vez posee características avanzadas para usuarios con un mayor grado de experiencia[24] .

Figura 2 Escáner de puertos interfaz gráfica



Fuente: Elaboración propia

Es una herramienta muy versátil, adicional al descubrimiento de puertos de comunicación abiertos también nos brinda la posibilidad de recopilar información

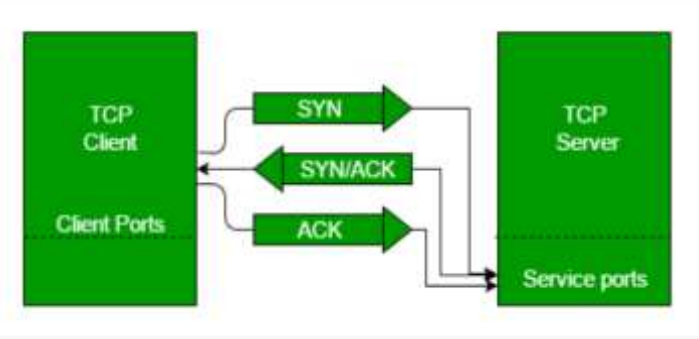
[24] NMAP.ORG. [sitio web]. [Consultado: 13 de febrero de 2023]. Disponible en: https://nmap.org/

sobre el estado y filtros de *firewall*; entre sus principales características podemos encontrar:

- Soporta protocolos HTTP y HTTPS
- Realiza escaneos de forma programada
- Soporta protocolo SSL

Nmap puede realizar escaneos de un único host o un rango de direcciones, su escaneo se basa en realizar peticiones TCP, ICMP, UDP entre otras, es importante que al utilizar esta herramienta se tenga un conocimiento básico sobre los protocolos de transporte que para el caso más utilizado TCP/IP es un protocolo de tres pasos, una llamada a un puerto en un destino remoto que se denomina SYN, una respuesta de parte del equipo remoto SYN-ACK si el puerto está abierto y a la escucha o RST si por el contrario el puerto se encuentra cerrado y por último el ACK enviado desde el equipo local hacia el equipo remoto, este proceso se conoce común mente como *Hand Shake*, este es el proceso sobre el cual la herramienta basa su funcionamiento para identificar que puertos de comunicación se encuentran abiertos en un host[25].

Figura 3 Establecimiento de una conexión TCP/IP



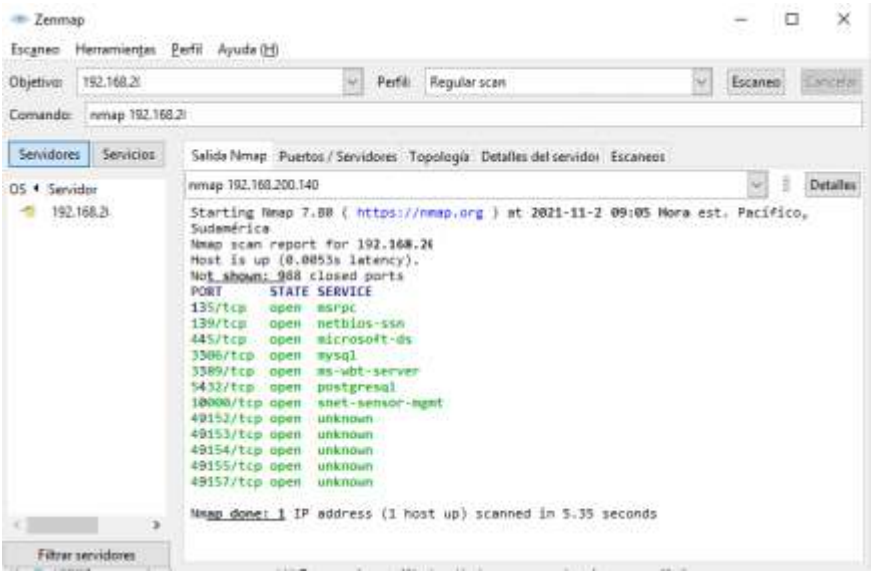
Fuente: GEEKFORGEEKS, TCP 3-way Handshake process. 2021. Disponible en: https://www.geeksforgeeks.org/tcp-3-way-handshake-process/

Un escaneo simple con la herramienta sin utilizar ningún tipo de filtros ya entrega unos datos iniciales sobre los puertos abiertos, lo que de por sí ya es un punto de análisis inicial, puesto que sin importar si el servicio que está a la escucha detrás del puerto enumerado este totalmente actualizado o parchado con esta información e posible lanzar un ataque de fuerza bruta basado en diccionario con usuarios y contraseñas por defecto, esto es posible aun cuando el servicio se encuentre a la escucha en un puerto diferente al que por lo general utiliza, ya que la herramienta mediante los procesos de *fingerprint* es capaz de detectar el tipo de servicio y su

[25] ECHEVERRÍA USÚA, Javier. Hacking ético: identificación de servicios con nmap [en línea]. VIAFIRMA. 14 de octubre de 2019. [Consultado: 3 de marzo de 2023]. Disponible en: https://www.viafirma.com/blog-xnoccio/es/identificacion-servicios-nmap/

versión; por esta razón es muy importante nunca dejar contraseñas por defecto en servidores, bases de datos, *routers* etc[26] .

Figura 4 Escaneo Regular



Fuente: Elaboración propia

6.1.2 *GREENBONE*

Esta herramienta permite la detección de diferentes tipos de problemas o vulnerabilidades tanto leves como graves según su sitio oficial la herramienta cuenta con aproximadamente 50.000 pruebas y datos de vulnerabilidades conocidas, este número aumenta día a día gracias a los aportes de su comunidad y los expertos de la empresa, posee una interfaz gráfica amigable para el usuario[27].

Esta herramienta cuenta con varias funciones que la hacen muy versátil, entre ellas podemos encontrar:

- Test Autenticados
- Test Anónimos
- Utiliza protocolos de alto y bajo nivel
- Permite realizar ajustes de rendimiento para exploraciones

Es importante destacar que esta herramienta pertenece al área de escáneres de vulnerabilidades que como se dijo anteriormente nos permite realizar validaciones

[26] COMPILAR NEWS. Comandos Nmap con ejemplos [blog]. 1 de marzo de 2021. [Consultado: 8 de abril de 2023]. Disponible en: https://conpilar.es/comandos-nmap-con-ejemplos/

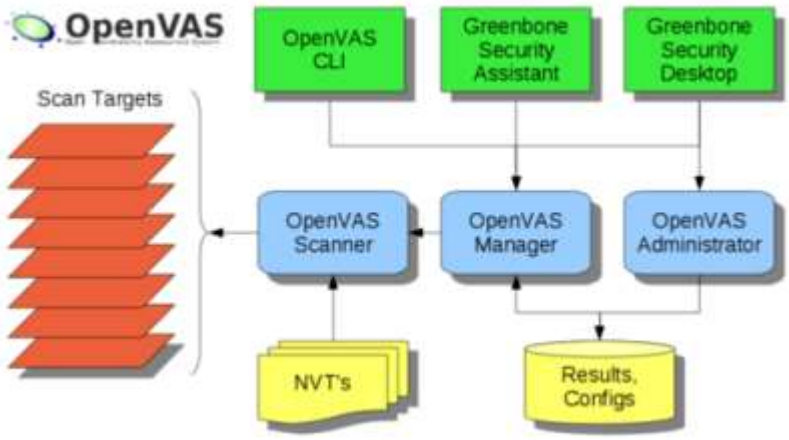
[27] ALTUBE VERA, Rafael. Qué es OpenVAS [blog]. Openwebinars. 11 de noviembre de 2020. [Consultado: 14 de diciembre de 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

en nuestro sistema operativo como en la red donde él se encuentra, su gran diferencia es que al contrario de un escáner de red que únicamente logra detectar puertos abiertos y servicios asociados a estos, *Greenbone* mediante el uso de un variado arsenal de protocolos y pruebas va un paso más allá y logra encontrar fallas potenciales o vulnerabilidades que pueden ser blanco de ataque de un delincuente cibernético.

El funcionamiento básico de la herramienta se basa en cuatro componentes principales:[28]

- ***Scanner*:** este servicio se encarga de realizar los escaneos sobre los servidores o equipos objetivo
- **Cliente Web:** es su interfaz gráfica, desde esta se realiza las operaciones de configuración de la herramienta, se ejecutan los análisis o se presentan los resultados
- ***Manager*:** Se encarga de interconectar todos los módulos anteriores y da la posibilidad de integrar nuevos módulos si se requieren.
- **Almacén de datos:** base de datos en la cual se almacenan los resultados de las pruebas para realizar análisis posteriores o identificar tendencias.

Figura 5 Esquema trabajo *Greenbone*



Fuente: Adaptado de: Estructura Greenbone. 2020 disponible en: https://kinomakino.blogspot.com/2014/03/

El portal de acceso a la herramienta es el cliente web a través de este se logra interactuar con los servicios *Greenbone Scanner y Greenbone Mannager* este último servicio se encarga de llevar a cabo las tareas de clasificación o filtrado de

[28] ÁLVAREZ HUERTA, Leopoldo. OpenVas en Linux: Explorando nuestros sistemas [blog]. Openwebinars. 30 de mayo de 2014. [Consultado: 14 de diciembre de 2022]. Disponible en: https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

los resultados obtenidos en los análisis, controla la base de datos de configuración y de resultados, administra los niveles de acceso de los usuarios y programa los escaneos de forma automática entre otras tareas. De otro lado el servicio *Greenbone scanner* es el encargado de ejecutar lo que se conoce como NVT (*Network Vulnerability Test*), estas pruebas tienen un numero de rutinas que pueden identificar la presencia de alguna vulnerabilidad o problema potencial en un sistema[29].

6.1.3 OWASP ZAP (*Zed Attack Proxy*)

Es un escáner de vulnerabilidades enfocado en servicios web es una herramienta de código abierto y es soportado por una comunidad internacional que trabaja para día a día mejorar la herramienta, es multiplataforma siendo soportada por sistemas operativos Windows, MacOs y Linux en sus versiones de 32 y 64 bits.

Esta herramienta de seguridad permite que se puedan auditar diferentes tipos de aplicaciones web mediante una serie de análisis y funciones específicas, mediante la instalación de un proxy que se encargará de realizar una captura de todas las peticiones es posible realizar un análisis detalla de estas, también brinda la posibilidad de localizar recursos en un servidor, realizar análisis pasivos, en las últimas versiones se ha incluido la posibilidad de usar tarjetas inteligentes como DNIe.

Hay que mencionar que las vulnerabilidades de una aplicación web pueden ser encontradas en todos sus componentes esto incluye los sistemas operativos sobre los cuales están alojadas, estos también presentan brechas de seguridad es por esto que es necesario realizar un análisis de vulnerabilidades integral que cubra todos los aspectos de un aplicación o sitio web[30].

Este escáner se basa en los datos consignados en el Top 10 de Owasp que es un documento que enmarca los diez riesgos de seguridad más importantes respecto a aplicaciones web, este listado se actualiza cada 3 años como se observa en la tabla 1, con base en los datos recopilados por especialistas en seguridad informática, en la siguiente tabla se puede observar el cambio de los riesgos respecto al año de publicación de la lista.

---

[29] MENDOZA, Miguel Ángel. Cómo utilizar OpenVAS para la evaluación de vulnerabilidades [blog]. Welivesecurity. 18 de noviembre de 2014. [Consultado: 14 de febrero de 2023]. Disponible en: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

[30] ASENCIO MENDOSA, Martha y MORENO PATIÑO, Pedro Julián. Desarrollo de una propuesta Metodológica para Determinar la Seguridad en una Aplicación. Trabajo de investigación Ingeniero de Sistemas y Computación. Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería Sistemas y Computación. 2011. 79 p. [Consultado: 10 de diciembre de 2022]. Disponible en: https://repositorio.utp.edu.co/server/api/core/bitstreams/f4d085e0-d12b-49f8-80aa-ea62228b18b6/content

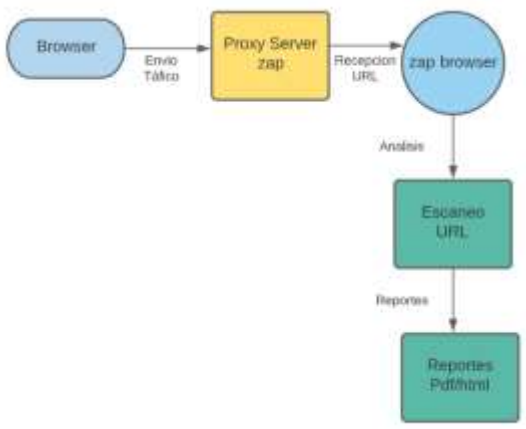
Tabla 1 Top 10 Owasp 2021 vs 2017

Top 10 - 2021	Top 10 - 2017
A01 – Broken Access Control	A01 – Injection
A02 - Cryptographic Failures	A02 – Broken Authentication
A03 - Injection	A03 - Sensitive Data Exposure
A04 - Insecure Design	A04 – XML External Entities (XXE)
A05 - Security Misconfiguration	A05 - Broken Access Control
A06 - Vulnerable and Outdated Components	A06 - Security Misconfiguration
A07 - Identification and Authentication Failures	A07 – Cross--Site--Scripting (XSS)
A08 - Software and Data Integrity Failures	A08 – Insecure Deserialization
A09 - Security Logging and Monitoring Failures	A09 – Using Components with Known Vulnerabilities
A10 - Server-Side Request Forgery	A10 – Insufficient Logging and Monitoring

Fuente: Elaboración propia

Owasp Zap como se puede ver en la figura 5, al momento de realizar un análisis, crea un servidor **PROXY** y el tráfico del sitio **WEB** analizado es pasado a través de este, en este punto vemos la importancia de los escaneos automáticos ya que estos nos ayudan a detectar las vulnerabilidades del sitio o aplicación web.

Figura 6 Flujo análisis Owasp Zap



Fuente: Adaptado de: cómo funciona ZAP. 2019. Disponible en: https://es.myservername.com/owasp-zap--tutorial--comprehensive-review--owasp-zap-tool

Para un uso efectivo de la herramienta es necesario tener en claro algunos conceptos y como estos se utilizan.

Break Points: Permiten que una solicitud realizada desde un navegador sea interceptada y modificada antes de ser enviada hacia la aplicación que se está analizando

Explorar: utilizar el navegador de la aplicación para explorar toda la aplicación web, activar botones, seguir vínculos enviar formularios entre otros.

***Spider*:** explorador de URL ocultas o rotas, permite también capturar los vínculos generados de forma dinámica.

Escaneo Activo: análisis de vulnerabilidades automático que se utiliza para encontrar debilidades sencillas.

Para lograr encontrar vulnerabilidades más complejas es necesario que se realicen pruebas manuales sobre la aplicación web, para este propósito es una buena práctica utilizar la guía de pruebas OWASP[31].

6.2 LEVANTAMIENTO DE INFORMACION INICIAL

Con el fin de que las pruebas de vulnerabilidad sean objetivas y entreguen resultados los más precisos posible es necesario contar con un listado o inventario detallado de las plataformas sobre las cuales se realizaran los análisis, para el presente proyecto se enfocarán las pruebas en los ambientes web de la Unidad Administrativa Especial de Servicios Públicos, los cuales constan de 4 servidores distribuidos entre servidores web y bases de datos.

6.2.1 Inventario de servidores

El inventario de servidores se realiza teniendo en cuenta aspectos netamente de hardware los cuales son importantes para lograr identificar vulnerabilidades asociadas a obsolescencia tecnológica o temas relacionados con ausencia de soporte de parte del fabricante.

En la tabla 2 podemos apreciar el inventario detallado de los servidores que serán objeto de análisis, en su totalidad se trata de máquinas virtuales del tipo Hyper-V. este tipo de servidores virtuales permiten que sea posible la aplicación de medidas de *hardening* de una forma ágil y segura ya que el despliegue de estas medidas se realiza de forma automática y centralizada desde un solo gestor o administrador de

[31] CABALLERO QUEZADA, Alonso Eduardo. ZAP. OWASP Zed Attack Proxy [Webinar]. mayo de 2016. [Consultado: 12 de noviembre de 2023]. Disponible en: https://www.slideshare.net/reydes/webinar-owasp-zed-attack-proxy-zap

hipervisores, de la tabla también es posible determinar que los ambientes con los que cuenta la entidad son iguales por tal motivo es posible realizar un primer despliegue en ambientes de pruebas o desarrollo, validar su correcto funcionamiento y posteriormente realizar el despliegue en ambientes de producción de tal forma que los servicios no se vean afectados.

Tabla 2 inventario de servidores

Servidor	Procesador	RAM	NIC	Tipo	Fabricante
Persefone1	64 núcleos	256 Gb	10GBbps	Host Físico	HPe
Persefone2	64 núcleos	256 Gb	10GBbps	Host Físico	HPe
Icaro	4 núcleos	8.0 Gb	10 Gbps	Máquina Virtual	Microsoft
Icaro_dll	4 núcleos	4.0 Gb	10 Gbps	Máquina Virtual	Microsoft
Cronos	4 núcleos	4.0 Gb	10 Gbps	Máquina Virtual	Microsoft
Cronos-dll	4 núcleos	8.0 Gb	10 Gbps	Máquina Virtual	Microsoft

Fuente: Elaboración propia

En la tabla 2 también se puede observar que la infraestructura virtual esta soportada por dos servidores físicos los cuales se encuentran configurados en un esquema de alta disponibilidad compuesto por dos nodos los cuales están administrados por el rol cluster de protección contra errores nativo del sistema operativo Windows, estos dos nodos cuentan con un almacenamiento compartido configurado en RAID 6 que soporta una tolerancia a fallos de dos discos en simultaneo, esta configuración garantiza que los servidores virtuales cuenten con una alta tolerancia a fallas físicas asegurando de esta manera la continua prestación de los servicios que las máquinas virtuales están soportando.

6.2.2 Inventario de aplicaciones

Poseer un listado completo de aplicaciones y servicios activos en cada uno de los servidores es de vital importancia a la hora de establecer que puertos de comunicaciones deben estar habilitados y cuales no, por otra parte, este listado permitirá la identificación de posible software no autorizado instalado en los servidores a analizar, por otro lado este inventario servirá de línea base para el análisis de los resultados obtenidos mediante las diferentes herramientas que se utilizaran en el presente proyecto

En las tablas 3 y 4 se puede observar que existen varios puertos abiertos de los cuales dos corresponden a servicio web en protocolo HTTP y HTTPS así como dos más son de servicio FTP, sobre este servicio se conocen varias vulnerabilidades sobre las cuales es necesario trabajar de tal forma que el servicio sea lo más seguro posible, es recomendable utilizar protocolo SFTP a cambio del FTP que se evidencia.

Tabla 3 Aplicaciones servidor web producción

Servidor: “Icaro” Rol: Servidor Web Producción	
Aplicación o servicio	**Puerto de comunicaciones asociado**
Servidor web IIS	80,443
Servidor FTP	21,22
Conexiones escritorio remoto	3390
Agente Zabbix	10050
Agente Fusión Inventory	62354
End Point	61617
Conexión VNC Server	5900

Fuente: Elaboración propia

Tabla 4 Aplicaciones servidor web desarrollo

Servidor: “Icaro_dll” Rol: Servidor Web Desarrollo	
Aplicación o servicio	**Puerto de comunicaciones asociado**
Servidor web IIS	80,443
Servidor FTP	21,22
Conexiones escritorio remoto	3389
Agente Zabbix	10050
Agente Fusión Inventory	62354
End Point	61617
Conexión VNC Server	5900

Fuente: Elaboración propia

Las tablas 5 y 6 evidencian la existencia de puertos a la escucha con servicios asociados de base de datos (3306) y un servicio de conexiones remotas RDP (3390), este protocolo de administración remota es conocido por presentar múltiples debilidades las que se deben tener presente al momento de realizar tareas de *hardening*, con el fin de evitar afectaciones por tener este servicio activado. Teniendo en cuenta que el acceso remoto por protocolo RDP es una herramienta esencial para la administración de los servidores es importante realizar un cambio en el puerto por defecto de este protocolo o efectuar tareas de ocultamiento mediante el uso de listas de acceso de tal manera que solo los usuarios autorizados puedan hacer uso de este método de conexión.

Tabla 5 Aplicaciones servidor base de datos producción

Servidor: “Cronos” Rol: Servidor base de datos producción	
Aplicación o servicio	**Puerto de comunicaciones asociado**
Base de datos MySQL	3306
Conexiones escritorio remoto	3390
Agente Zabbix	10050
Agente Fusión Inventory	62354
End Point	61617
Conexión VNC Server	5900

Fuente: Elaboración propia

Tabla 6 Aplicaciones servidor base de datos desarrollo

Servidor: “Cronos_dll” Rol: Servidor base de datos desarrollo	
Aplicación o servicio	**Puerto de comunicaciones asociado**
Base de datos MySQL	3306
Conexiones escritorio remoto	3389
Agente Zabbix	10050
Agente Fusión Inventory	62354
End Point	61617
Conexión VNC Server	5900

Fuente: Elaboración propia

De las tablas anteriores también se puede evidenciar la existencia de un servicio de acceso remoto VNC en puerto 5900, este es el puerto por defecto de este servicio por lo que sería muy fácil para un atacante intentar vulnerar esa conexión conociendo las vulnerabilidades del servicio VNC, es importante que estos puertos por defecto sean cambiados a puertos personalizados de tal forma que sea más difícil para un atacante el poder enumerar los servicios que se encuentran a la escucha en los servidores.

6.3 PRUEBAS DE COMPORTAMIENTO DE HERRAMIENTAS Y ANÁLISIS DE VULNERABILIDADES

De acuerdo con los lineamientos establecidos en la metodología propuesta en el presente proyecto las pruebas de vulnerabilidad se realizarán teniendo en cuenta tres aspectos principales:

- Verificación de puertos abiertos y servicios o aplicaciones en escucha, esta prueba se realizará utilizando la herramienta NMAP y tendrá como objetivo los cuatro servidores detallados en la tabla 2

- Análisis de vulnerabilidades prueba realizada mediante la herramienta *Greenbone* y tendrá como objetivo los cuatro servidores detallados en la tabla 2.

- Pruebas de vulnerabilidad sobre aplicaciones web, se desarrollan mediante la herramienta OWASP ZAP y serán objeto de esta únicamente los dos servidores web relacionados en la tabla 2

6.3.1 Verificación de puertos

La verificación de puertos abiertos en los servidores se realizará mediante la herramienta Nmap, haciendo uso de su interfaz gráfica mediante los comandos de escaneo completo de todos los puertos TCP/IP.

Después de realizar la prueba, en el apartado de reconocimiento se encuentra que el escaneo detectó que el servidor tiene un sistema operativo Windows 2012 R2 y 34 puertos abiertos de un total de 65535.

Figura 7 *Fingerprint* servidor

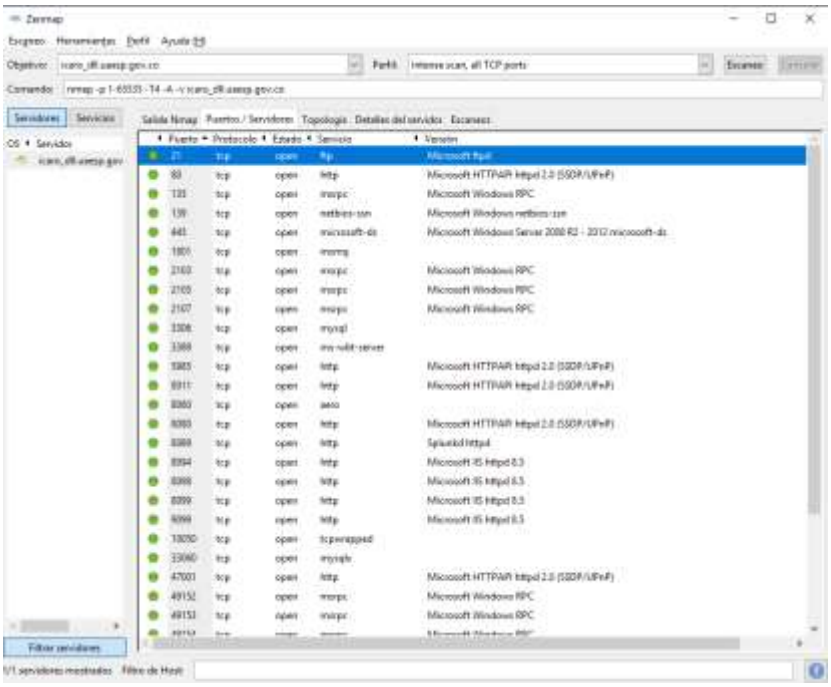
Fuente: elaboración propia

El siguiente paso es verificar los servicios asociados a los puertos abiertos que se detectaron

En la figura 7 se observa que existe un gran número de puertos abiertos principalmente se observa que existe un servicio FTP plano en el puerto 21 y un servicio HTTP en puerto 80, estos dos protocolos se consideran inseguros ya que el tráfico se encuentra plano de tal manera que un atacante podría llegar a interceptar este flujo de información y obtener datos sensibles de la organización. También se observa que existen puertos abiertos diferentes al 80 relacionados con el servidor web IIS y con protocolo HTTP lo cual es un indicador de que en ese servidor existen varios sitios web todos recibiendo peticiones en tráfico plano lo que constituye que para un atacante la superficie de acción es mucho más amplia y por consiguiente el porcentaje de éxito de un ataque se ve aumentado de manera significativa.

De igual forma existen puertos abiertos con protocolo de ejecución de comandos remotos RCP, sobre estos no se observa ningún servicio asociado razón por la cual es necesario identificar cada uno de los puertos que aceptan este protocolo e identificar qué servicio hace uso de ellos de tal forma que sea posible desactivar los que no sean estrictamente necesarios para la correcta operación de los servicios reduciendo de esta forma el área de ataque.

Figura 8 Resultados de análisis



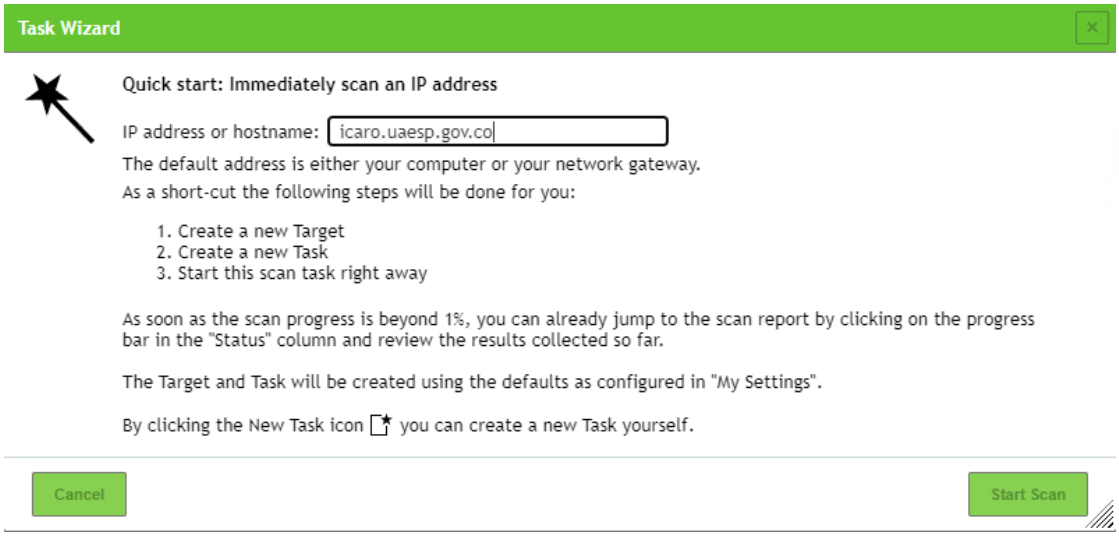
Fuente: elaboración propia

6.3.2 Análisis de vulnerabilidades

Las pruebas de vulnerabilidades se realizarán de forma controlada sin afectar los servicios de los equipos objeto del análisis mediante la herramienta Greenbone.

Para iniciar las pruebas de vulnerabilidad es necesario ingresar a la consola web de administración mediante el usuario y contraseña configurado previamente durante la instalación del software. Desde la plataforma de administración web se debe ejecutar el asistente para configurar el escaneo, de esta forma se crearán todas las tareas necesarias y el análisis iniciará de forma inmediata, para este paso solo se debe especificar la dirección ip o nombre de host del servidor objetivo.

Figura 9 Asistente para nuevo análisis



Fuente elaboración propia

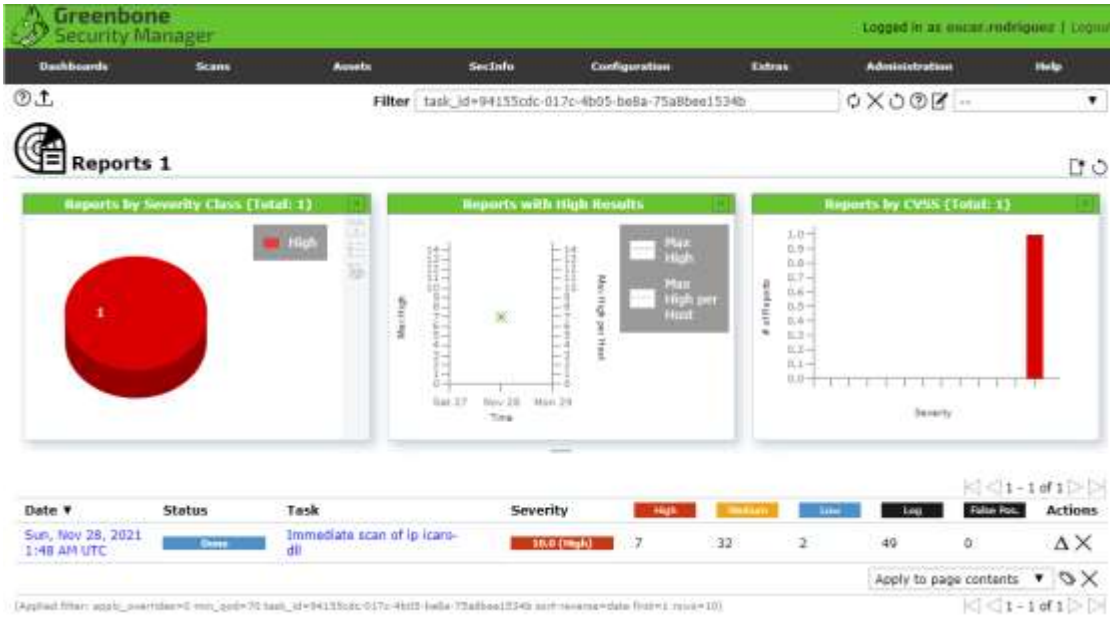
Al finalizar el proceso de creación de la nueva tarea el escaneo da inicio y puede tardar algunos minutos dependiendo de los recursos de hardware de la máquina que lanza el análisis, si se desea desde la plataforma en la pestaña de tareas se puede verificar el porcentaje de avance.

Figura 10 Proceso de análisis

Fuente elaboración propia

Al finalizar el escaneo de las vulnerabilidades, el reporte ya estará disponible en la plataforma, este se puede visualizar de dos formas una general en la cual solo se mostrará las vulnerabilidades encontradas y su clasificación de acuerdo con su criticidad.

Figura 11 Resultados generales del análisis



Fuente elaboración propia

La segunda forma de visualización es más detallada, con información más concreta sobre el tipo de vulnerabilidad encontrada, la herramienta clasifica la severidad de la vulnerabilidad encontrada en una escala de 1 a 10 siendo 10 el nivel más alto de criticidad.

Figura 12 Resultados detallados de análisis

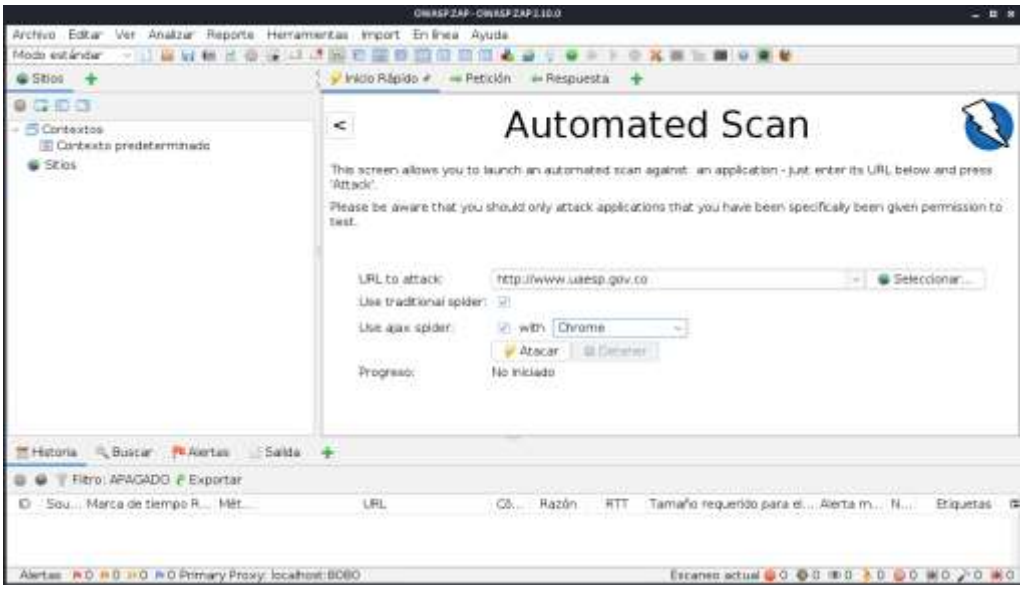
Fuente elaboración propia

6.3.3 Análisis de aplicaciones web

La Unidad Administrativa Especial de Servicios Públicos cuenta en su infraestructura con un portal web en el cual se concentra toda la información de interés general referente a recolección de basuras y planes de reciclaje, este portal será el objetivo del presente análisis, el cual se desarrollará utilizando la herramienta OWASP ZAP.

Una vez se tenga ingreso a la consola de trabajo de la herramienta se debe especificar la dirección URL del sitio o aplicación web que se desea analizar es recomendable activar la opción de utilizar "*ajax spider*" para poder obtener los vínculos dinámicos que pudieren existir en la aplicación.

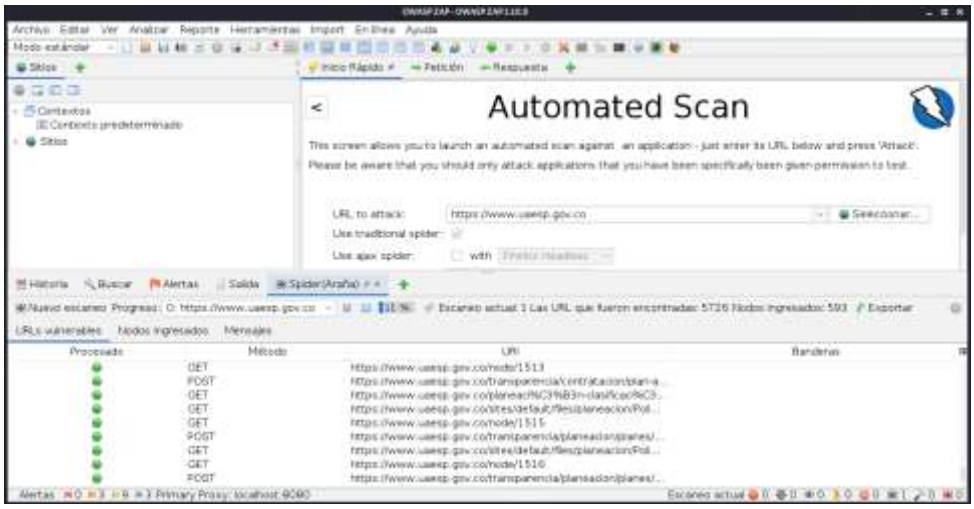
Figura 13 Lanzamiento análisis OWASP



Fuente elaboración propia

Después de iniciado el análisis debemos esperar algún tiempo hasta que este finalice, este tiempo dependerá en gran medida de la complejidad del sitio o aplicación web que se esté analizando, podemos ver en la pestaña Spider el progreso de la tarea.

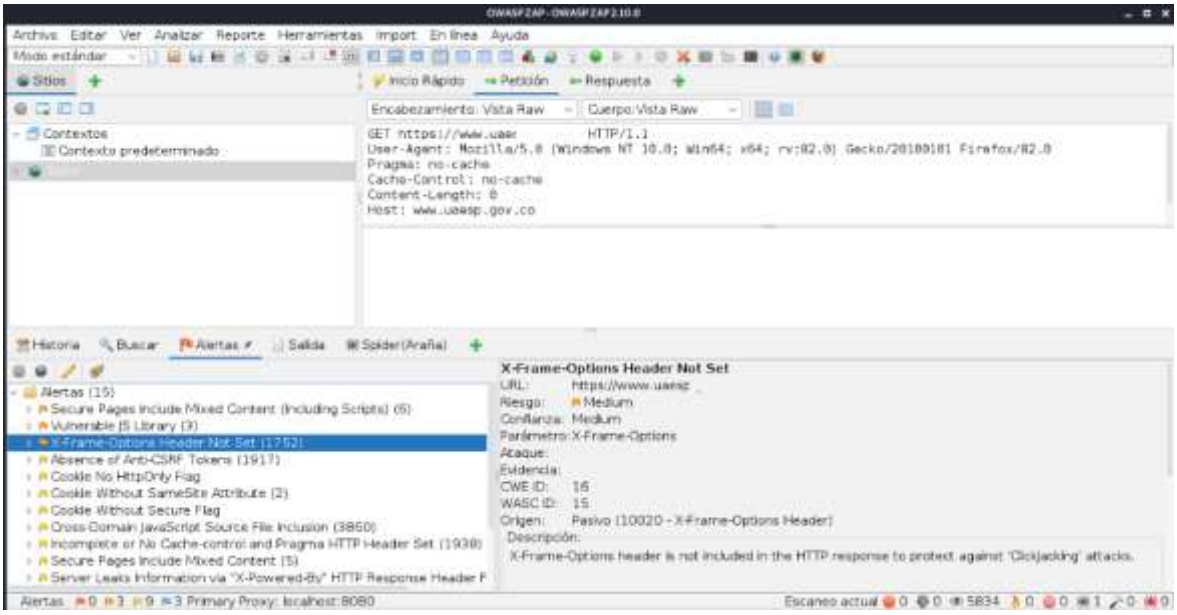
Figura 14 Progreso de análisis



Fuente elaboración propia

Al finalizar el escaneo se podrá observar en la pestaña de alertas un listado de todas las vulnerabilidades detectadas, estas estarán clasificadas en alta, media o baja de acuerdo con el nivel de riesgo que estas presenten en la aplicación web analizada.

Figura 15 Informe de resultados



Fuente elaboración propia

6.4 ANÁLISIS DE RESULTADOS

A continuación, se detalla el resultado consolidado de los resultados obtenidos después de realizar el análisis con las herramientas mencionadas anteriormente.

6.4.1 Escaneo de puertos

Con base en los resultados obtenidos después de realizar el escaneo de puertos abiertos obtiene 4 tablas en las cuales se consolida la información relevante sobre el número de puerto su estado el servicio que está a la escucha y la versión de este, esta información al ser contrastada con el inventario inicial de aplicaciones aprobadas para cada servidor plantea un panorama claro del estado de aseguramiento del servidor objeto de análisis.

En la tabla 7 es posible observar los puertos abiertos detectados en el servidor web de producción, en esta se puede observar un total de 34 puertos de los cuales dos (135,139) son utilizados por el sistema operativo para los protocolos de carpetas compartidas SMB, 9 están identificados en el inventario inicial de aplicaciones instaladas en el servidor y los restantes 23 no se encuentran identificados en los listados de la entidad, de estos se puede observar que la mayoría hacen referencia al servicios de "*Microsoft Remote Procedure Call*" (msrpc) este protocolo se utiliza con mucha frecuencia para realizar procesos de manera remota sobre el servidor, por lo cual el hecho de que se encuentren abiertos y no estén controlados presenta un grave riesgo de seguridad.

Tabla 7 Puertos Abiertos Servidor Web producción

Servidor ICARO			
PORT	**STATE**	**SERVICE**	**VERSION**
21/tcp	Open.	ftp	Microsoft ftpd
80/tcp	Open.	http	Microsoft IIS webserver 8.5
135/tcp	Open.	msrpc	Microsoft Windows RPC
139/tcp	Open.	netbios-ssn	
443/tcp	Open.	ssl/http	Microsoft IIS webserver 8.5
445/tcp	Open.	netbios-ssn	
1025/tcp	Open.	msrpc	Microsoft Windows RPC
1026/tcp	Open.	msrpc	Microsoft Windows RPC
1027/tcp	Open.	msrpc	Microsoft Windows RPC
1028/tcp	Open.	msrpc	Microsoft Windows RPC
1029/tcp	Open.	msrpc	Microsoft Windows RPC
1037/tcp	Open.	msrpc	Microsoft Windows RPC
2105/tcp	Open.	msrpc	Microsoft Windows RPC
2107/tcp	Open.	msrpc	Microsoft Windows RPC
3389/tcp	Open.	microsoft-rdp	Microsoft Terminal Service
5985/tcp	Open.	http	Microsoft HTTPAPI. httpd 2.0.

Tabla 8 (Continuación)

Servidor ICARO			
PORT	**STATE**	**SERVICE**	**VERSION**
6183/tcp	Open.	msrpc	Microsoft Windows RPC
6184/tcp	Open.	unknown	
8021/tcp	Open.	http	Microsoft HTTPAPI httpd. 2.0.
8022/tcp	Open.	http	Microsoft IIS webserver 8.5
8090/tcp	Open.	http	Microsoft HTTPAPI httpd. 2.0.
9091/tcp	Open.	http	Microsoft IIS webserver 8.5
9395/tcp	Open.	unknown	
10000/tcp	Open.	snet-sensor-mgmt	
10050/tcp	Open.	tcpwrapped	
11731/tcp	Open.	msrpc	Microsoft Windows RPC
47001/tcp	Open.	http	Microsoft HTTPAPI httpd. 2.0.
48634/tcp	Open.	msrpc	Microsoft Windows RPC
48672/tcp	Open.	msrpc	Microsoft Windows RPC
48678/tcp	Open.	msrpc	Microsoft Windows RPC
62354/tcp	Open.	tcpwrapped	

Fuente: Elaboración Propia

Por su parte la tabla 8 presenta un comportamiento similar de 34 puertos encontrados 11 son reconocidos y deben estar abiertos los restantes 23 no deberían estarlo, en este caso se presenta una situación particular y es que los puertos encontrados son exactamente iguales a los encontrados en el ambiente de producción, al realizar un análisis más afondo se encontró que esto se debe a que el ambiente de desarrollo se creó a partir de una copia fiel del ambiente de producción

Tabla 9 Puertos Abiertos Servidor Web Desarrollo

Servidor ICARO_DLL			
PORT	**STATE**	**SERVICE**	**VERSION**
21/tcp.	Open.	ftp	Microsoft ftpd
80/tcp.	Open.	http	Microsoft IIS webserver 8.5
135/tcp.	Open.	msrpc	Microsoft Windows RPC
139/tcp.	Open.	netbios-ssn	
443/tcp.	Open.	ssl/http	Microsoft IIS webserver 8.5
445/tcp.	Open.	netbios-ssn	
1025/tcp.	Open.	msrpc	Microsoft Windows RPC

Tabla 10 (Continuación)

Servidor ICARO_DLL			
PORT	**STATE**	**SERVICE**	**VERSION**
1026/tcp.	Open.	msrpc	Microsoft Windows RPC
1027/tcp.	Open.	msrpc	Microsoft Windows RPC
1028/tcp.	Open.	msrpc	Microsoft Windows RPC
1029/tcp.	Open.	msrpc	Microsoft Windows RPC
1037/tcp.	Open.	msrpc	Microsoft Windows RPC
1801/tcp.	Open.	unknown	
2103/tcp.	Open.	msrpc	Microsoft Windows RPC
2105/tcp.	Open.	msrpc	Microsoft Windows RPC
2107/tcp.	Open.	msrpc	Microsoft Windows RPC
3389/tcp.	Open.	microsoft-rdp	Microsoft Terminal Service
5985/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0
6160/tcp.	Open.	msrpc	Microsoft Windows RPC
6183/tcp.	Open.	msrpc	Microsoft Windows RPC
6184/tcp.	Open.	unknown	
8021/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0
8022/tcp.	Open.	http	Microsoft IIS webserver 8.5
8090/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0
9091/tcp.	Open.	http	Microsoft IIS webserver 8.5
9395/tcp.	Open.	unknown	
10000/tcp.	Open.	snet-sensor-mgmt	
10050/tcp.	Open.	tcpwrapped	
11731/tcp.	Open.	msrpc	Microsoft Windows RPC
47001/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0
48634/tcp.	Open.	msrpc	Microsoft Windows RPC
48672/tcp.	Open.	msrpc	Microsoft Windows RPC
48678/tcp.	Open.	msrpc	Microsoft Windows RPC
62354/tcp.	Open.	tcpwrapped	

Fuente: Elaboración Propia

Se observa que en el servidor analizado se encuentra abiertos y a la escucha varios puertos, todos ellos asociados al protocolo de ejecución remota de Microsoft RPC, este protocolo es utilizado por el sistema operativo para realizar tareas de ejecución de comandos de forma remota es por esta razón que el hallazgo de estos puertos abiertos representa un riesgo importante en la seguridad del servidor puesto que existen vulnerabilidades conocidas en este protocolo las cuales pueden ser explotadas por un atacante logrando comprometer de forma significativa los servicios alojados en el servidor, la existencia de ese gran número de puertos

abiertos también puede significar que el servidor ni se encuentre protegido por un servicio de firewall local o si este se encuentra instalado está en estado desactivado, esta situación conlleva a que el sistema operativo presente un alto riesgo de verse comprometido ante un ataque.

Por otra parte se evidencia que existen varios portales o aplicaciones web que están a la escucha mediante protocolo HTTP en puertos diferentes al 80, si bien es cierto esta práctica es común en ambientes de desarrollo, se debe prestar especial atención ya que el uso de comunicaciones sin cifrar presenta un riesgo de robo de información o lo que puede llegar a ser más grave, robo de credenciales de acceso, por este motivo es necesario que los puertos que se utilizan para estas conexiones estén a la escucha de forma local y no remota de esta manera se logra reducir en gran manera el riesgo de esta práctica sin afectar los servicios asociados.

La tabla 9 presenta la lista de puertos encontrados en el servidor de base de datos ambiente de producción, en esta tabla se observa que existen 20 puertos abiertos de los cuales 8 están dentro del inventario inicial de aplicaciones lo que deja 12 puertos abiertos sin control y sin conocimiento de estos por parte de la oficina de TI, en este análisis se observa nuevamente que la gran mayoría de los puertos no inventariados tienen el protocolo MSRCP asociado, como se observó en las tablas 7 y 8.

Tabla 11 Puertos Abiertos Servidor Base de Datos Producción

Servidor CRONOS			
PORT	**STATE**	**SERVICE**	**VERSION**
80/tcp.	Open.	http	Microsoft IIS webserver 8.5
135/tcp.	Open.	msrpc	Microsoft Windows RPC
139/tcp.	Open.	netbios-ssn	
443/tcp.	Open.	ssl/http	Microsoft IIS webserver 8.5
445/tcp.	Open.	netbios-ssn	
1025/tcp.	Open.	msrpc	Microsoft Windows RPC
1026/tcp.	Open.	msrpc	Microsoft Windows RPC
1027/tcp.	Open.	msrpc	Microsoft Windows RPC
1028/tcp.	Open.	msrpc	Microsoft Windows RPC
1029/tcp.	Open.	msrpc	Microsoft Windows RPC
1030/tcp.	Open.	msrpc	Microsoft Windows RPC
3306/tcp.	Open.	mysql	MySQL 5.7.13-log
3389/tcp.	Open.	microsoft-rdp	Microsoft Terminal Service
4118/tcp.	Open.	ssl/unknown	
5985/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

Fuente: Elaboración Propia

Del análisis de los resultados presentados en la tabla 9 se puede evidenciar que existe una marcada tendencia a dejar puertos abiertos que utilizan el protocolo RCP generando un grave riesgo ya que este puerto puede ser utilizado por un atacante para ejecutar instrucciones o comandos de forma remota, de igual manera se evidencia que existe una mala práctica consistente en no activar el firewall local del sistema operativo.

En la Tabla 10 se observa que los puertos detectados en el servidor de base de datos de desarrollo son los mismos que se encontraron en el servidor de base de datos de producción nuevamente porque el ambiente de desarrollo se creó a partir de una copia fiel del ambiente de producción.

Tabla 12 Puertos Abiertos Servidor Base de Datos Desarrollo

Servidor CRONOS_DLL			
PORT	**STATE**	**SERVICE**	**VERSION**
80/tcp.	Open.	http	Microsoft IIS webserver 8.5
135/tcp.	Open.	msrpc	Microsoft Windows RPC
139/tcp.	Open.	netbios-ssn	
443/tcp.	Open.	ssl/http	Microsoft IIS webserver 8.5
445/tcp.	Open.		netbios-ssn
1025/tcp.	Open.	msrpc	Microsoft Windows RPC
1026/tcp.	Open.	msrpc	Microsoft Windows RPC
1027/tcp.	Open.	msrpc	Microsoft Windows RPC
1028/tcp.	Open.	msrpc	Microsoft Windows RPC
1029/tcp.	Open.	msrpc	Microsoft Windows RPC
1030/tcp.	Open.	msrpc	Microsoft Windows RPC
3306/tcp.	Open.	mysql	MySQL 5.7.13-log
3389/tcp.	Open.	ms-term-serv	
4118/tcp.	Open.	ssl/unknown	
5985/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0
10050/tcp.	Open.	tcpwrapped	
47001/tcp.	Open.	http	Microsoft HTTPAPI httpd 2.0
47712/tcp.	Open.	msrpc	Microsoft Windows RPC
47714/tcp.	Open.	msrpc	Microsoft Windows RPC
62354/tcp.	Open.	tcpwrapped	

Fuente: Elaboración Propia

Las tablas anteriores muestran un panorama claro de la situación de los servidores analizados, en los resultados encontrados se evidencia que tanto los servidores de ambientes de producción como los de desarrollo no cuentan con un control estricto de las comunicaciones entrantes y salientes de igual forma la entidad cuenta con un inventario de aplicaciones y puertos admitidos en estos ambientes pero este

listado no se aplica ya que existen una gran cantidad de puertos abiertos que no están relacionados dentro de los puertos y aplicaciones que se marcan como aplicaciones permitidas.

Por otro lado, al realizar el análisis de los servidores se logra evidenciar que ninguno de ellos cuenta con un sistema cortafuegos activado lo que representa un alto riesgo ya que si bien la entidad cuenta con sistemas de firewall perimetral que logran proteger los servidores de ataques externos no existe un método de protección ante un ataque que tenga su origen en la red local o que provenga de un usuario que haya sido víctima de alguna campaña de phishing.

Por lo anteriormente expuesto es recomendable que se implementen políticas de activación de sistemas de firewall local de tal forma que se cuente con una capa adicional de protección contra ataques internos.

6.4.2 Escaneo de Vulnerabilidades

Aparte de los puertos abiertos que se pudieren encontrar en un servidor y que se consideran brechas de seguridad, es importante prestar atención a otro ítem que muchas veces pasa desapercibido pero que tiene un impacto mucho mayor en los niveles de seguridad este ítem se refiere a las vulnerabilidades presentes en el sistema operativo y aplicaciones adicionales instaladas en un servidor.

La herramienta utilizada para realizar este análisis nos entrega resultados en los cuales es posible observar el código CVE de la vulnerabilidad encontrada, el puntaje CVSS el cual va de 0 a 100 siendo 100 el valor más alto y por este motivo de mayor impacto, también se encuentran datos adicionales como el nivel de severidad de la vulnerabilidad y el nombre común de esta.

En la tabla 11 se puede observar el resultado del escaneo realizado sobre el servidor web ambiente de producción, este análisis arroja un total de 47 vulnerabilidades descubiertas las cuales todas presentan un nivel de severidad alto y puntajes CVSS en un rango de 70 a 100, esta situación de acuerdo con la clasificación total generada por la herramienta ubica a este servidor con un puntaje de 10 en la severidad de lo encontrado lo cual es un riesgo muy elevado para un servidor que se encuentra en un ambiente de producción, por otro lado la tabla muestra que la gran mayoría de vulnerabilidades descubiertas tiene que ver con la versión del Framework PHP instalado que para este caso es la versión 7.0, con base en esta situación se puede inferir que este servidor se encuentra bajo el control de un sistema de actualizaciones automáticas de sistema operativo (WSUS), o existe una política de actualización de parches de seguridad que se ejecuta con frecuencia ya que no se evidencian vulnerabilidades relacionados con sistema operativo.

Tabla 13 Vulnerabilidades Servidor Web producción

Servidor ICARO			
CVEs	**CVSS**	**Severity**	**NVT Name**
	100	High	PHP End Of Life Detection (Windows)
	100	High	PHP End Of Life Detection (Windows)
CVE-2017-9120	98	High	PHP Integer Overflow Vulnerability Aug18 (Windows)
CVE-2019-13224	98	High	PHP CVE-2019-13224 Use-After-Free Vulnerability (Windows)
CVE-2016-10166,CVE-2019-9020	98	High	PHP Multiple Vulnerabilities (Feb 2019) - Windows
CVE-2016-10166,CVE-2019-9020	98	High	PHP Multiple Vulnerabilities (Feb 2019) - Windows
CVE-2017-9120	98	High	PHP Integer Overflow Vulnerability Aug18 (Windows)
CVE-2021-21708	98	High	PHP < 7.4.28, 8.0.x. < 8.0.16, 8.1.x. < 8.1.3 Security Update (Feb 2022) - Windows
CVE-2018-7584	98	High	PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)
CVE-2021-21708	98	High	PHP < 7.4.28, 8.0.x. < 8.0.16, 8.1.x. < 8.1.3 Security Update (Feb 2022) - Windows
CVE-2019-9637,CVE-2019-9638	98	High	PHP Multiple Vulnerabilities - Mar19 (Windows)
CVE-2018-7584	98	High	PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)
CVE-2019-9637,CVE-2019-9638	98	High	PHP Multiple Vulnerabilities - Mar19 (Windows)
CVE-2019-13224	98	High	PHP CVE-2019-13224 Use-After-Free Vulnerability (Windows)
CVE-2020-7059,CVE-2020-7060	91	High	PHP < 7.2.27, 7.3.x < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)
CVE-2020-7059,CVE-2020-7060	91	High	PHP < 7.2.27, 7.3.x. < 7.3.14, 7.4.x < 7.4.2 Multiple Vulnerabilities - Jan20 (Windows)
CVE-2018-10549,CVE-2018-10546	88	High	PHP Multiple Vulnerabilities May18 (Windows)
CVE-2018-10549,CVE-2018-10546	88	High	PHP Multiple Vulnerabilities May18 (Windows)
CVE-2022-31625,CVE-2022-31626	81	High	PHP < 7.4.30, 8.0.x. < 8.0.20, 8.1.x. < 8.1.7 Security Update (Jun 2022) - Windows

Tabla 14 (Continuación)

CVEs	CVSS	Servidor ICARO Severity	NVT Name
CVE-2022-31625,CVE-2022-31626	81	High	PHP < 7.4.30, 8.0.x < 8.0.20, 8.1.x < 8.1.7 Security Update (Jun 2022) - Windows
CVE-2016-2183,CVE-2016-6329	75	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
CVE-2018-19935	75	High	PHP CVE-2018-19935 - imap_mail Denial of Service Vulnerability (Windows)
CVE-2018-19935	75	High	PHP CVE-2018-19935 - imap_mail Denial of Service Vulnerability (Windows)
	75	High	phpinfo() output Reporting
	75	High	phpinfo() output Reporting
	75	High	phpinfo() output Reporting
	75	High	phpinfo() output Reporting
CVE-2016-2183,CVE-2016-6329,CVE-2020-12872	75	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
CVE-2017-7189	75	High	PHP CVE-2017-7189 Improper Input Validation Vulnerability (Windows)
CVE-2017-7189	75	High	PHP CVE-2017-7189 Improper Input Validation Vulnerability (Windows)
CVE-2020-7067	75	High	PHP < 7.2.30, 7.3. < 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)
CVE-2020-7067	75	High	PHP < 7.2.30, 7.3 .< 7.3.17, 7.4 < 7.4.5 DoS Vulnerability - Apr20 (Windows)
CVE-2020-8169	75	High	PHP < 7.2.32, 7.3. < 7.3.20, 7.4. < 7.4.8 libcurl Vulnerability - May20 (Windows)
CVE-2020-8169	75	High	PHP < 7.2.32, 7.3. < 7.3.20, 7.4. < 7.4.8 libcurl Vulnerability - May20 (Windows)
CVE-2021-21702	75	High	PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Windows
CVE-2021-21702	75	High	PHP < 7.3.27, 7.4.x < 7.4.15, 8.0.x < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Windows
CVE-2019-9022	75	High	PHP Memory Disclosure Vulnerability (Windows)
CVE-2019-9022	75	High	PHP Memory Disclosure Vulnerability (Windows)

Tabla 11 (Continuación)

Servidor ICARO			
CVSS	Severity		NVT Name
CVE-2018-14851,CVE-2018-14883,CVE-2018-15132	75	High	PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Windows)
CVE-2018-14851,CVE-2018-14883,	75	High	PHP Multiple Heap Buffer Overflow and Information Disclosure Vulnerabilities (Windows)
CVE-2018-19518,CVE-2018-20783	75	High	PHP Multiple Vulnerabilities - Dec18 (Windows)
CVE-2018-19518,CVE-2018-20783	75	High	PHP Multiple Vulnerabilities - Dec18 (Windows)
CVE-2019-11041,CVE-2019-11042	71	High	PHP Multiple Vulnerabilities - Aug19 (Windows)
CVE-2019-11041,CVE-2019-11042	71	High	PHP Multiple Vulnerabilities - Aug19 (Windows)
CVE-2021-21703	70	High	PHP 5.3.7 - 7.3.31, 7.4.x. < 7.4.25, 8.0.x. < 8.0.12 Security Update (Oct 2021) - Windows
CVE-2021-21703	70	High	PHP 5.3.7 - 7.3.31, 7.4.x. < 7.4.25, 8.0.x. < 8.0.12 Security Update (Oct 2021) - Windows

Fuente: elaboración propia

En la anterior tabla se observa que el análisis detecto un gran número de debilidades asociadas a él *framework* PHP, la gran mayoría de estas presentan un impacto alto y se evidencia su causa raíz en la versión de esta plataforma 5.3 para algunos portales y 7.0 para otros, estas dos versiones se consideran obsoletas y ya no tienen respaldo de parte de fabricante, esta situación genera un grave riesgo ya que existe gran cantidad de *exploits* que son efectivos sobre esas versiones generando que el servidor de producción pueda ser fácilmente atacado mediante técnicas de inyección de código que pueden poner en riesgo la integridad de la información contenida en ellos, ante esta situación es recomendable establecer planes de actualizaciones sobre los portales web de tal manera que estos se encuentren en la medida de lo posible utilizando las últimas versiones estables de PHP.

La Tabla 12 presenta los resultados obtenidos en el análisis realizado al servidor web en ambiente de desarrollo, en esta se observa que existen 5 vulnerabilidades

con puntajes CVS entre 40 y 50, esta situación ubica a este servidor en un rango de severidad de 5.0 lo que corresponde a severidad media, este servidor a pesar de ser una copia del ambiente de producción no presenta las vulnerabilidades asociadas al *Framework* PHP ver 7.0 esto se debe a que en este servidor se encuentra instalada la versión 8.1lacual es la última versión estable liberada hasta la fecha de realización del análisis.

Tabla 15 Vulnerabilidades Servidor Web Desarrollo

Servidor ICARO_DLL			
CVEs	**CVSS**	**Severity**	**NVT Name**
CVE-2013-2566,CVE-2015-2808,CVE-2015-4000	50	Medium	SSL/TLS: Report Weak Cipher Suites
	50	Medium	DCE/RPC and MSRPC Services Enumeration Reporting
CVE-2011-3389,CVE-2015-0204	43	Medium	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
	40	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
	40	Medium	SSLTLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Fuente: elaboración propia

La anterior tabla presenta cinco vulnerabilidades descubiertas en el sistema operativo del servidor de desarrollo, en la tabla se observa que existen dos vulnerabilidades de impacto medio con un puntaje CVSS de 50 la primera hace referencia a una vulnerabilidad conocida que impacta el protocolo de transporte SSL/TLS en este servidor se encuentra haciendo uso de protocolos de encriptación débiles, esto podría llegar a permitir a un atacante obtener información al realizar un proceso de cifrado reverso.

De igual manera se detecta una vulnerabilidad asociada al protocolo RCP esta vulnerabilidad es importante ya que en los análisis anteriores se detectó la existencia de un alto número de puertos que están a la escucha de este protocolo, por esta razón esta debilidad deberá ser mitigada a la menor brevedad posible ya que representa una alta posibilidad de que un atacante pueda llegar a explotar esta vulnerabilidad y lograr obtener control del servidor.

En la Tabla 13 se observan los resultados del análisis realizado sobre el servidor de base de datos en ambiente de producción este servidor presenta 4 vulnerabilidades las cuales tienen un puntaje CVSS entre 40 y 50 puntos esto ubica a este equipo en

un nivel de severidad o compromiso medio en comparación con los otros análisis se puede observar que el nivel de compromiso es el más bajo y las vulnerabilidades descubiertas no son de criticidad alta, este escenario es alentador dado el rol que este servidor ejecuta y la criticidad de la información que en él se almacena, sin embargo es importante tener en cuenta que en este servidor se están utilizando protocolos TLS 1.0 y TLS 1.1 los cuales son antiguos y por buenas prácticas no se deben utilizar, es recomendable en la medida de lo posible deshabilitaros y utilizar la versión 1.3.

Tabla 16 Vulnerabilidades Servidor Base de Datos Producción

Servidor CRONOS			
CVEs	**CVSS**	**Severity**	**NVT Name**
CVE-2013-2566,CVE-2015-2808,CVE-2015-4000	50	Medium	SSL/TLS: Report Weak Cipher Suites
	50	Medium	DCE/RPC and MSRPC Services Enumeration Reporting
CVE-2011-3389,CVE-2015-0204	43	Medium	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
	40	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Fuente: Elaboración propia

La tabla 14 plasma los resultados obtenidos después del análisis realizado sobre el servidor de base de datos en ambiente de desarrollo, en ella se observa un total de 15 vulnerabilidades descubiertas con puntajes CVSS entre 75 y 34 esto ubica a este servidor en un nivel de compromiso alto con un puntaje total de 7.5, es recomendable realizar una revisión general sobre los protocolos SSL y TLS en este servidor ya que la gran mayoría de reportes del análisis están asociados a estos.

Nuevamente se observa que en el servidor denominado cronos existe una vulnerabilidad asociada al protocolo RCP la que permite que un atacante logre obtener información sobre el tipo de servidor, sistema operativo entre otros, esta información puede ser utilizada por un ciberdelincuente para intentar realizar ataques más estructurados, además es importante recalcar que en la etapa de análisis de puertos abiertos se evidencio que existen varios puertos que utilizan este protocolo lo cual aumenta sustancialmente el nivel de criticidad de esta debilidad, es recomendable establecer políticas de actualización constante del sistema operativo con el fin de contar con los últimos parches que logren asegurar este tipo de protocolos, así como la implementación de políticas de bloqueo mediante firewall de sistema operativo.

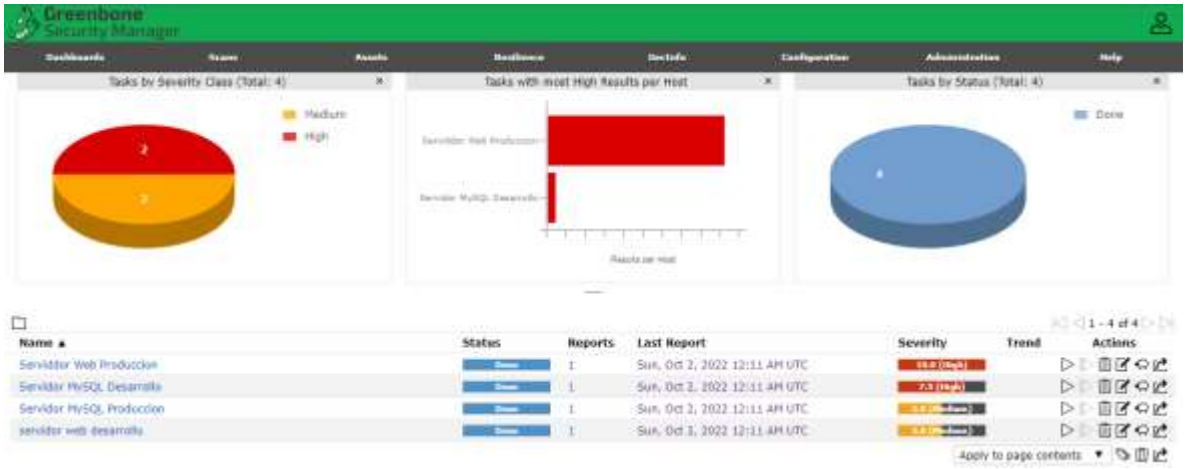
Tabla 17 Vulnerabilidades Servidor Base de Datos Desarrollo

Servidor CRONOS_DLL			
CVEs	**CVSS**	**Severity**	**NVT Name**
CVE-2016-2183,CVE-2016-6329,CVE-2020-12872	75	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
CVE-2016-2183,CVE-2016-6329,CVE-2020-12872	75	High	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
CVE-2016-0800,CVE-2014-3566	59	Medium	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
	50	Medium	SSL/TLS: Certificate Expired
	50	Medium	DCE/RPC and MSRPC Services Enumeration Reporting
CVE-2013-2566,CVE-2015-2808,CVE-2015-4000	50	Medium	SSL/TLS: Report Weak Cipher Suites
CVE-2013-2566,CVE-2015-2808,CVE-2015-4000	50	Medium	SSL/TLS: Report Weak Cipher Suites
CVE-2011-3389,CVE-2015-0204	43	Medium	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection.
CVE-2011-3389,CVE-2015-0204	43	Medium	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection
	40	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability.
	40	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability.
	40	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability.
	40	Medium	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm.
	40	Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability.
CVE-2014-3566	34	Low	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability. (POODLE)

Fuente: Elaboración propia

La figura 15 presenta la valoración general de estado de compromiso de los servidores web al momento de realizar el análisis en ella se puede observar que el servidor del ambiente de producción presenta un puntaje elevado en el nivel de criticidad de las vulnerabilidades encontradas, esta situación se considera muy riesgosa ya que existen múltiples vectores de ataque y los resultados de un ataque exitoso pueden comprometer en gran forma la información alojada en los portales web de la entidad.

Figura 16 Resumen de índice de criticidad



Fuente: Elaboración propia

En la figura 15 se observa un resumen de la situación de los cuatro servidores analizados, en el resumen se observa que el servidor con el mayor grado de compromiso corresponde al servidor de aplicaciones de ambiente de producción, este tiene un puntaje de 10.0 el cual es el puntaje máximo de la escala de compromiso, este es un indicador de que los servicios web alojados en dicho servidor se encuentran en un grave riesgo, ya que para un atacante puede ser muy fácil lograr acceso a este elemento y realizar cambios no autorizado o en el peor de los casos afectar la correcta prestación de los servicios, por este motivo es importante priorizar las acciones tendientes a asegurar este dispositivo logrando que su puntaje de compromiso sea mucho menor que el actual, para lograr este objetivo es necesario que se implementen políticas de actualización constante de tal manera que el sistema operativo cuente siempre con los últimos parches de seguridad liberados, también es necesario que se establezcan normas o políticas de mejora continua y actualización de los portales web de tal manera que para este caso particular sea posible el paso de versiones antiguas de PHP a las versiones actuales que cuentan con soporte de parte de fabricante.

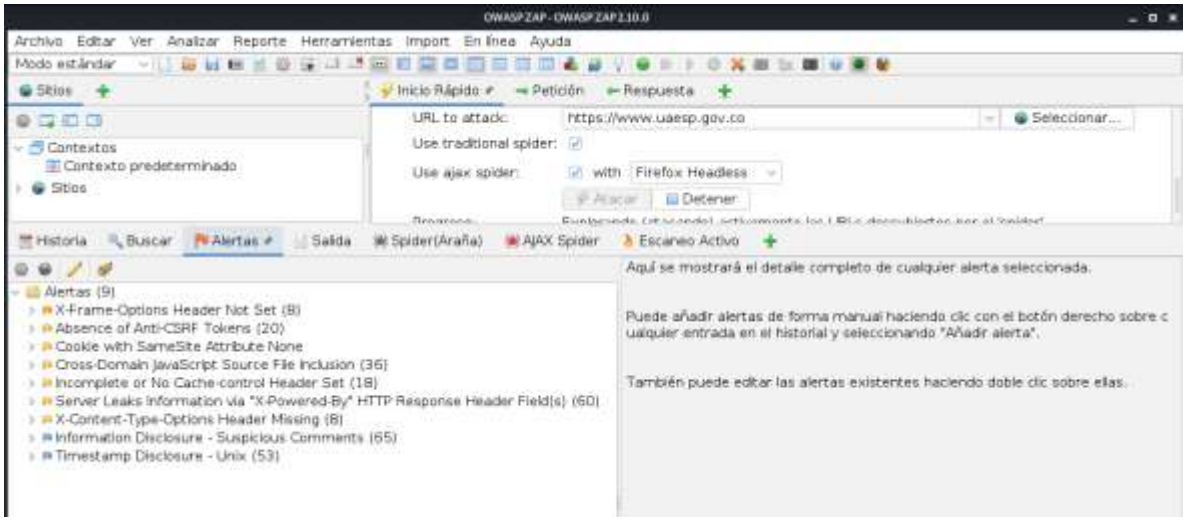
6.4.3 Escaneo Aplicación web

Adicional al escaneo de puertos y vulnerabilidades en la capa de servidores, se realiza un escaneo del portal web con el fin de encontrar vulnerabilidades

específicas de sitios web, esta clasificación se realiza teniendo en cuenta el Top 10 OWASP.

La figura 16 muestra el resultado del análisis de vulnerabilidades realizado sobre el sitio web, en dicho resultado se observa que existen un total de 9 alertas distribuidas por nivel de criticidad así: 0 de impacto crítico, 0 de impacto alto, 1 de impacto medio, 6 de impacto bajo y 2 catalogadas como informacionales.

Figura 17 Escaneo OWASP



Fuente: Elaboración propia

Teniendo en cuenta los resultados del análisis, se observa que el portal web no presenta un compromiso alto sin embargo existe una vulnerabilidad que es importante destacar y es la correspondiente al encabezado *X-Frame-Options* el cual no está habilitado en las respuestas HTTP, esta situación puede permitir que se secuestre la página web en un *frame* ubicado en un servido malicioso y de esta manera interceptar el tráfico entre los usuarios y el portal web de la entidad

6.4.4 Salvaguardas Propuestas

En la tabla No. 15 se detalla el resultado de los análisis de seguridad realizados y las soluciones o salvaguardas a implementar para minimizar el riesgo de una posible explotación de una vulnerabilidad, en la tabla se observa que la gran mayoría de salvaguardas hacen referencia a actualizaciones sobre el *framework* PHP , teniendo en cuenta que la última versión liberada de PHP al momento de la elaboración del presente análisis es la es la 8.0 el saldo desde versiones antiguas como 5.3 o 7.1 es de un alto impacto e implica acciones adicionales como modificación de código ya que existen muchos métodos que debido a su inseguridad ya no se utilizan en las nuevas versiones razón por la cual al realizar simplemente la actualización de PHP existe una alta posibilidad de que los portales se vean afectados y queden inoperantes.

Por este motivo es importante que se diseñe un plan de actualización en el cual se dé prelación a las modificaciones en código necesarias para que los portales sean operativos en la nueva versión de PHP, todas estas modificaciones deben ser realizadas inicialmente en los ambientes de pruebas de tal forma que el servicio de producción no se vea afectado.

Tabla 18 Salvaguardas Propuestas

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	100	PHP End Of Life Detection (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..80010 09)	Una versión antigua de PHP no recibe ninguna actualización de seguridad de parte del proveedor. Por este motivo las vulnerabilidades de seguridad no corregidas podrían ser aprovechadas por un atacante para comprometer la seguridad de este host.	Actualizar la versión de PHP en el servidor a una versión soportada por el fabricante		Icaro (servidor Web Producción)
Alta	98	PHP Integer Overflow Vulnerability Aug18 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..80010 09)	La explotación exitosa de esta vulnerabilidad permitirá a los atacantes provocar una denegación de servicio al realizar un desbordamiento de enteros y, por lo tanto, bloquear la aplicación.	No existen ninguna solución conocida al menos desde hace un año de la divulgación de esta vulnerabilidad. Las opciones de solución generales son actualizar a una más nueva de PHP liberar, deshabilitar las funciones respectivas.	CVE-2017-9120	Icaro (servidor Web Producción)

Tabla 19 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	98	PHP CVE-2019-13224 Use-After-Free Vulnerability (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)	Esta falla permite a los atacantes causar potencialmente la divulgación de información, la negación de servicio, o posiblemente ejecución de código proporcionando una expresión regular diseñada.	Actualice a la versión 7.1.32, 7.3.9 o posterior.	CVE-2019-13224	Icaro (servidor Web Producción)
Alta	98	PHP Multiple Vulnerabilities (Feb 2019) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 5.6.40, 7.1.16, 7.2.14, 7.3.1 o posterior.	CVE-2016-10166, CVE-2019-9020, CVE-2019-9021, CVE-2019-9023, CVE-2019-9024, CVE-2019-6977	Icaro (servidor Web Producción)
Alta	98	PHP < 7.4.28, 8.0.x < 8.0.16, 8.1.x < 8.1.3 Security Update (Feb 2022) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.4.28, 8.0.16, 8.1.3 o posterior.	CVE-2021-21708	Icaro (servidor Web Producción)

Tabla 20 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	98	PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0…800109)	La explotación de esta vulnerabilidad permitirá a un atacante ejecutar código arbitrario en el contexto de la aplicación afectada.	Actualización a la versión 7.2.3, 7.0.28, 5.6.34, 7.1.15 o posterior.	CVE-2018-7584	Icaro (servidor Web Producción)
Alta	98	PHP Multiple Vulnerabilities - Mar19 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.1.27, 7.2.16, 7.3.3 o posterior.	CVE-2019-9637 CVE-2019-9638 CVE-2019-9639	Icaro (servidor Web Producción)
Alta	98	PHP Stack Buffer Overflow Vulnerability Mar18 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)	La explotación exitosa permitirá ejecutar código arbitrario en el contexto de la aplicación afectada. Los intentos de explotación fallidos darán lugar a condiciones de denegación de servicio.	Actualización a la versión 7.2.3, 7.0.28, 5.6.34, 7.1.15 o posterior.	CVE-2018-7584	Icaro (servidor Web Producción)

Tabla 21 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	98	PHP CVE-2019-13224 Use-After-Free Vulnerability (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)	Esta falla permite a los atacantes causar potencialmente la divulgación de información, la denegación de servicio, o posiblemente ejecución de código proporcionando una expresión regular.	Actualice a la versión 7.1.32, 7.3.9 o posterior.	CVE-2019-13224	Icaro (servidor Web Producción)
Alta	91	PHP < 7.2.27, 7.3.x. < 7.3.14, 7.4.x. < 7.4.2. Multiple Vulnerabilities - Jan20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.2.27, 7.3.14, 7.4.2 o posterior.	CVE-2020-7059,CVE-2020-7060	Icaro (servidor Web Producción)
Alta	88	PHP Multiple Vulnerabilities May18 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)	La explotación exitosa permitirá a un atacante llevar a cabo ataques XSS, bloquear PHP, llevar a cabo denegación de servicio y ejecutar código arbitrario en el contexto de la aplicación afectada.	Actualice a la versión 7.2.5 o 7.0.30 o 5.6.36 o 7.1.17 o posterior.	CVE-2018-10549,CVE-2018-10546,CVE-2018-10548,CVE-2018-10547	Icaro (servidor Web Producción)

Tabla 22 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	81	PHP < 7.4.30, 8.0.x. < 8.0.20, 8.1.x. < 8.1.7. Security Update (Jun 2022) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.4.30, 8.0.20, 8.1.7 o posterior.	CVE-2022-31625,CVE-2022-31626	Icaro (servidor Web Producción)
Alta	75	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	SSL/TLS: Report Weak Cipher Suites OID: 1.3.6.1.4.1..25623.1.0..103440		La configuración de estos servicios se debe cambiar para que ya no acepte los conjuntos de cifrado enumerados. Consulte las referencias para obtener más recursos que lo apoyen con esta tarea.	CVE-2016-2183,CVE-2016-6329,CVE-2020-12872	Icaro (servidor Web Producción)
Alta	75	PHP CVE-2018-19935 - imap_mail Denial of Service Vulnerability (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)	La explotación exitosa permitirá a los atacantes provocar una denegación de servicio de la aplicación afectada.	Actualice a la versión 5.6.39, 7.0.33, 7.1.26, 7.2.14, 7.3.0 o posterior.	CVE-2018-19935	Icaro (servidor Web Producción)

Tabla 23 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	75	phpinfo() output Reporting	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)	Parte de la información que se puede recopilar de este archivo incluye: El nombre de usuario del usuario que ejecuta el proceso PHP, si es un usuario sudo , la dirección IP del host, la versión del servidor web, la versión del sistema (Unix, Linux, Windows, ...), y el directorio raíz del servidor web.	Elimine los archivos enumerados o restrinja el acceso a ellos.		Icaro (servidor Web Producción)
Alta	75	PHP CVE-2017-7189 Improper Input Validation Vulnerability (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1..0.800109)		El proveedor no puso a disposición ninguna solución. Opciones generales de solución son actualizar a una versión más reciente, deshabilitar las funciones respectivas, eliminar el producto o reemplazarlo por otro.	CVE-2017-7189	Icaro (servidor Web Producción)

Tabla 24 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	75	PHP < 7.2.30., 7.3 < 7.3.17, 7.4. < 7.4.5 DoS Vulnerability - Apr20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.2.30, 7.3.17, 7.4.5 o posterior.	CVE-2020-7067	Icaro (servidor Web Producción)
Alta	75	PHP < 7.2.32, 7.3 < 7.3.20., 7.4. < 7.4.8 libcurl Vulnerability - May20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.2.32, 7.3.20, 7.4.8 o posterior.	CVE-2020-8169	Icaro (servidor Web Producción)
Alta	75	PHP < 7.3.27, 7.4.x. < 7.4.15, 8.0.x. < 8.0.2 NULL Deference Vulnerability (Feb 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.3.27, 7.4.15, 8.0.2 o posterior.	CVE-2021-21702	Icaro (servidor Web Producción)
Alta	75	PHP Memory Disclosure Vulnerability. (Windows.)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.1.26, 7.2.14, 7.3.2 o posterior.	CVE-2019-9022	Icaro (servidor Web Producción)
Alta	75	PHP Multiple Heap Buffer Overflow and Information Disclosure, Vulnerabilities	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)	La explotación exitosa permitirá a los atacantes causar desbordamiento de buffer,	Actualización a PHP versión 5.6.37, 7.0.31, 7.1.20 o 7.2.8 o posterior.	CVE-2018-14851,CVE-2018-14883,CVE-2018-15132	Icaro (servidor Web Producción)

Tabla 25 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Alta	75	PHP Multiple Vulnerabilities - Dec18 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)	La explotación exitosa permitirá a los atacantes ejecutar código remoto en la aplicación/sistema afectado y/o causar denegación de servicio.	Actualice a la versión 5.6.39, 7.0.33, 7.1.25, 7.2.13, 7.3.0 o posterior.	CVE-2018-19518,CVE-2018-20783,CVE-2018-19395,CVE-2018-19396	Icaro (servidor Web Producción)
Alta	71	PHP Multiple Vulnerabilities - Aug19 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0..800109)		Actualice a la versión 7.1.31, 7.2.21, 7.3.8 o posterior.	CVE-2019-11041,CVE-2019-11042	Icaro (servidor Web Producción)
Alta	70	PHP 5.3.7 - 7.3.31, 7.4.x. < 7.4.25, 8.0.x. < 8.0.12. Security Update (Oct 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.3.32 (aún no publicada), 7.4.25, 8.0.12 o posterior	CVE-2021-21703	Icaro (servidor Web Producción)
Media	68	PHP Heap Use-After-Free Vulnerability - Sep19 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.1.32 o posterior.		Icaro (servidor Web Producción)
Media	68	PHP Multiple Vulnerabilities - Sep19 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.2.22, 7.3.9 o posterior.		Icaro (servidor Web Producción)
Media	65	PHP < 7.2.34, 7.3 < 7.3.23, 7.4 < 7.4.11.	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.2.34, 7.3.23, 7.4.11 o posterior.	CVE-2020-7069,CVE-2020-7070	Icaro (servidor Web Producción)

Tabla 26 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Media	65	PHP PHP-FPM Denial of Service Vulnerability (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)	La explotación exitosa permitirá a un atacante consumir el 100% de la CPU, y consumir espacio en disco con un gran volumen de registros de errores.	Actualice a PHP 7.1.20, 7.2.8 o 7.3.0alpha3.	CVE-2015-9253	Icaro (servidor Web Producción)
Media	65	PHP < 7.3.30, 7.4.x < 7.4.23, 8.0.x < 8.0.10 Security Update (Sep 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.3.31, 7.4.24, 8.0.11 o posterior.	CVE-2021-21706	Icaro (servidor Web Producción)
Media	65	PHP < 7.2.26 Multiple Vulnerabilities - Dec19 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1.25623.1.0.800109)		Actualice a la versión 7.2.26 o posterior.	CVE-2019-11046., CVE-2019-11045, CVE-2019-11044., CVE-2019-11050, CVE-2019-11047	Icaro (servidor Web Producción)
Media	65	PHP. < 7.2.34, 7.3. < 7.3.23, 7.4 < 7.4.1.1 Multiple Vulnerabilities - October20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.2.34, 7.3.23, 7.4.11 o posterior.	CVE-2020-7069,CVE-2020-7070	Icaro (servidor Web Producción)

Tabla 27 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Media	59	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection OID: 1.3.6.1.4.1..25623.1.0..111012	Un atacante podría utilizar los defectos criptográficos conocidos para espiar la conexión entre los clientes y el servicio para obtener acceso a datos confidenciales transferidos dentro de la conexión segura. Además, las vulnerabilidades descubiertas en estos protocolos no recibirán actualizaciones de seguridad.	Se recomienda deshabilitar SSLv2 y/o SSLv3 obsoletos y activar los protocolos TLSv1.2+.	CVE-2016-0800,CVE-2014-3566	Icaro (servidor Web Producción)
Media	54	PHP < 7.2.29 Multiple Vulnerabilities - Mar20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1..4.1.25623.1.0..800109)		Actualice a la versión 7.2.29 o posterior.	CVE-2020-7064,CVE-2020-7066	Icaro (servidor Web Producción)
Media	53	PHP < 7.2.31, 7.3 < 7.3.18, 7.4 < 7.4.6 Multiple DoS Vulnerabilities - May20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.2.31, 7.3.18, 7.4.6 o posterior.	CVE-2019-11048	Icaro (servidor Web Producción)

Tabla 28 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Media	53	PHP < 7.3.26, 7.4.x. < 7.4.14, 8.0.x. < 8.0.1 Filter Vulnerability (Jan 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.3.26, 7.4.14, 8.0.1 o posterior.	CVE-2020-7071	Icaro (servidor Web Producción)
Media	53	PHP < 7.3.29. Multiple Vulnerabilities (Jul 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.3.29 o posterior.	CVE-2021-21704,CVE-2021-21705	Icaro (servidor Web Producción)
Media	53	PHP < 7.2.28. Multiple Vulnerabilities - Feb20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.2.28 o posterior.	CVE-2020-7062,CVE-2020-7063	Icaro (servidor Web Producción)
Media	53	PHP < 7.3.33, 7.4.x < 7.4.26, 8.0.x < 8.0.13 Security Update (Nov 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.3.33, 7.4.26, 8.0.13 o posterior.	CVE-2021-21707	Icaro (servidor Web Producción)

Tabla 29 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Media	50	SSL/TLS: Report Weak Cipher Suites	SSL/TLS: Report Weak Cipher Suites OID: 1.3.6.1.4.1..25623.1.0.1.03440		La configuración de estos servicios debe cambiarse para que ya no acepta las suites de cifrado débiles.	CVE-2013-2566,CVE-2015-2808,CVE-2015-4000	Icaro (servidor Web Producción)
Media	50	SSL/TLS: Certificate Expired	SSL/TLS: Certificate Expired OID: 1.3.6.1.4.1..25623.1.0..103955		Reemplace el certificado SSL/TLS por uno nuevo.		Icaro (servidor Web Producción)
Media	50	PHP < 7.3.28, 7.4.x. < 7.4.18 IMAP Header Injection . Vulnerability (Apr 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4.1..25623.1.0..800109)		Actualice a la versión 7.3.28, 7.4.18 o posterior.		Icaro (servidor Web Producción)
Media	50	PHP < 7.3.30, 7.4.x. < 7.4.23, 8.0.x .< 8.0.10 Security Update (Aug 2021) - Windows	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.3.30, 7.4.23, 8.0.10 o posterior.		Icaro (servidor Web Producción)
Media	50	DCE/RPC and MSRPC Services Enumeration Reporting	DCE/RPC and MSRPC Services Enumeration Reporting OID: 1.3.6.1.4..1.25623.1.0..10736	Un atacante puede usar esta debilidad para obtener más información acerca del host remoto.	Filtre el tráfico entrante a estos puertos.		Icaro (servidor Web Producción)

Tabla 30 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Media	50	SSL/TLS: Report Weak Cipher Suites	SSL/TLS: Report Weak Cipher Suites OID: 1.3.6.1.4.1..25623.1.0.1.03440		La configuración de estos servicios se debe cambia para que no se acepten las suites de cifrado débiles.	CVE-2013-2566,CVE-2015-2808,CVE-2015-4000	Icaro (servidor Web Producción)
Media	47	PHP Security Bypass Vulnerability May18 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)	La explotación exitosa permitirá a un atacante eludir las restricciones de seguridad y acceder a datos de configuración confidenciales para otras cuentas directamente en la memoria del proceso de trabajo de PHP.	Actualice a la versión 7.2.4 o 7.0.29 o 5.6.35 o 7.1.16 o posterior.	CVE-2018-10545	Icaro (servidor Web Producción)
Media	43	SSL/TLS: Deprecated TLSv1.0. and TLSv1.1. Protocol Detection	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocols Detections OID: 1.3.6.1.4.1.25623.1.0.117274	Un atacante podría usar los defectos criptográficos conocidos para espiar la conexión entre los clientes y el servicio para obtener acceso a datos confidenciales transferidos dentro de la conexión segura.	Se recomienda deshabilitar el TLSv1.0 obsoleto y/o protocolos TLSv1.1 y activar los protocolos TLSv1.2+.	CVE-2011-3389,CVE-2015-0204	Icaro (servidor Web Producción)

Tabla 31 (Continuación)

Criticidad	Puntaje CVS	Vulnerabilidad	Método de detección	Impacto	Solución	Referencias	Servidores afectados
Media	40	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vu... OID: 1.3.6.1.4.1..25623.1.0.1.06223		Implementar curva elíptica de Diffie-Hellman (ECDHE) o usar un grupo Diffie-Hellman de 2048 bits o más fuerte. Para servidores web Apache: A partir de la versión 2.4.7., mod_ssl utilizará parámetros DH. que incluyen primos con longitudes de más de 1024 bits.		Icaro (servidor Web Producción)
Baja	36	PHP < 7.2.33.., 7.3 < 7.3.21, 7.4 < 7.4.9. DoS Vulnerability - August20 (Windows)	PHP Detection (HTTP) (OID: 1.3.6.1.4..1.25623.1.0..800109)		Actualice a la versión 7.2.33, 7.3.21, 7.4.9 o posterior.	CVE-2020-7068	Icaro (servidor Web Producción)
Baja	34	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulne... OID: 1.3.6.1.4.1.25623.1.0.802087	La explotación exitosa permitirá a los atacantes que hacen uso de la técnica de hombre en el medio obtener acceso al flujo de datos de texto sin formato.	Las posibles mitigaciones son: - Desactivar SSLv3 - Desactivar conjuntos de cifrado compatibles con los modos de cifrado CBC - Habilitar TLS_FALLBACK_SCSV si el servicio proporciona TLSv1.0+	CVE-2014-3566	Icaro (servidor Web Producción)

Fuente: Elaboración propia

6.5 ESTRATEGIAS DE HARDENING

Se deben establecer diferentes políticas de *hardening* en función del sistema o componente que se desea proteger, es fundamental que se intente ser lo más granular posible de tal manera que se logre abarcar la totalidad de elementos que hacen parte de un sistema.

Para realizar un proceso de *hardeninig* sobre los servidores objeto del presente análisis se tomaron en cuenta las buenas prácticas dictadas por el centro para la seguridad de Internet, CIS por sus siglas en Ingles *Center for Internet Security,* este es un organismo sin ánimo de lucro que lidera una comunidad global de profesionales en tecnología encargados de desarrollar y actualizar continuamente los estándares de seguridad para proporcionar lineamientos que ayuden a proteger de manera proactiva los sistemas contra amenazas emergentes.

Para lograr un *hardening* efectivo es importante que este plan de aseguramiento se realice teniendo en cuenta las tres siguientes etapas:

- **Pruebas**: aplicar políticas de endurecimiento sobre ambientes productivos puede llegar a causar traumatismos extensos en la operación de lo servicios, es por esta razón que antes de iniciar con el despliegue de cualquier tipo de política o cambio en la configuración de los servidores o sistemas de información, es necesario que estas políticas sean evaluadas en entornos que simulen de la manera más fiel el entorno de red y servidores que se encuentra en producción de esta forma será posible identificar que políticas pueden ser desplegadas sin riesgo de interrupción de lo servicios, cuales deben ser afinadas para asegurar los sistemas pero sin afectar su operación o cuales en definitiva por motivos de fuerza mayor no es posible desplegar en ambientes productivos.

- **Despliegue y cumplimiento**: El siguiente paso en la implementación de un esquema de endurecimiento es el despliegue de las políticas y configuraciones que fueron evaluadas y afinadas en la fase de pruebas, estas configuraciones debe ser desplegadas a la totalidad de componentes que hacen parte del sistema, esta etapa es altamente propensa a la aparición de errores humanos razón por la cual se recomienda que en esta etapa se haga uso de alguna herramienta de asistencia puesto que el garantizar que todas las reglas fueron desplegadas a la totalidad de elementos de forma correcta puede llegar a ser una tarea agobiante.

- **Monitoreo**: las redes de las organizaciones son dinámicas por lo que es necesario que estén en un constante proceso de monitoreo y supervisión de tal forma que sea posible reaccionar ante cambios en la configuración de servidores sin que estos hechos afecten los niveles de seguridad ya establecidos.

Con base en lo expresado anteriormente es importante que se cuente con un set de herramientas que ayuden al administrador a realizar cada una de las tres etapas del proceso de endurecimiento, estas herramientas se pueden clasificar en:

- **Herramientas de automatización de *hardening*** este tipo de herramientas brindan un completo esquema de solución realizando todo el proceso de pruebas, hacen uso de técnicas de *machine learning* para aprender sobre el comportamiento del sistema y de esta manera poder informar con un alto grado de certeza el impacto que un cambio de configuración presentará en la operación de los servicios, logrando reducir de esta manera el consumo de recursos requeridos para las fases de prueba.

  Estas herramientas también tienen la capacidad de realizar el despliegue de las políticas que fueron puestas a prueba sobre la totalidad de elementos que componen el sistema reduciendo de esta manera el error humano.

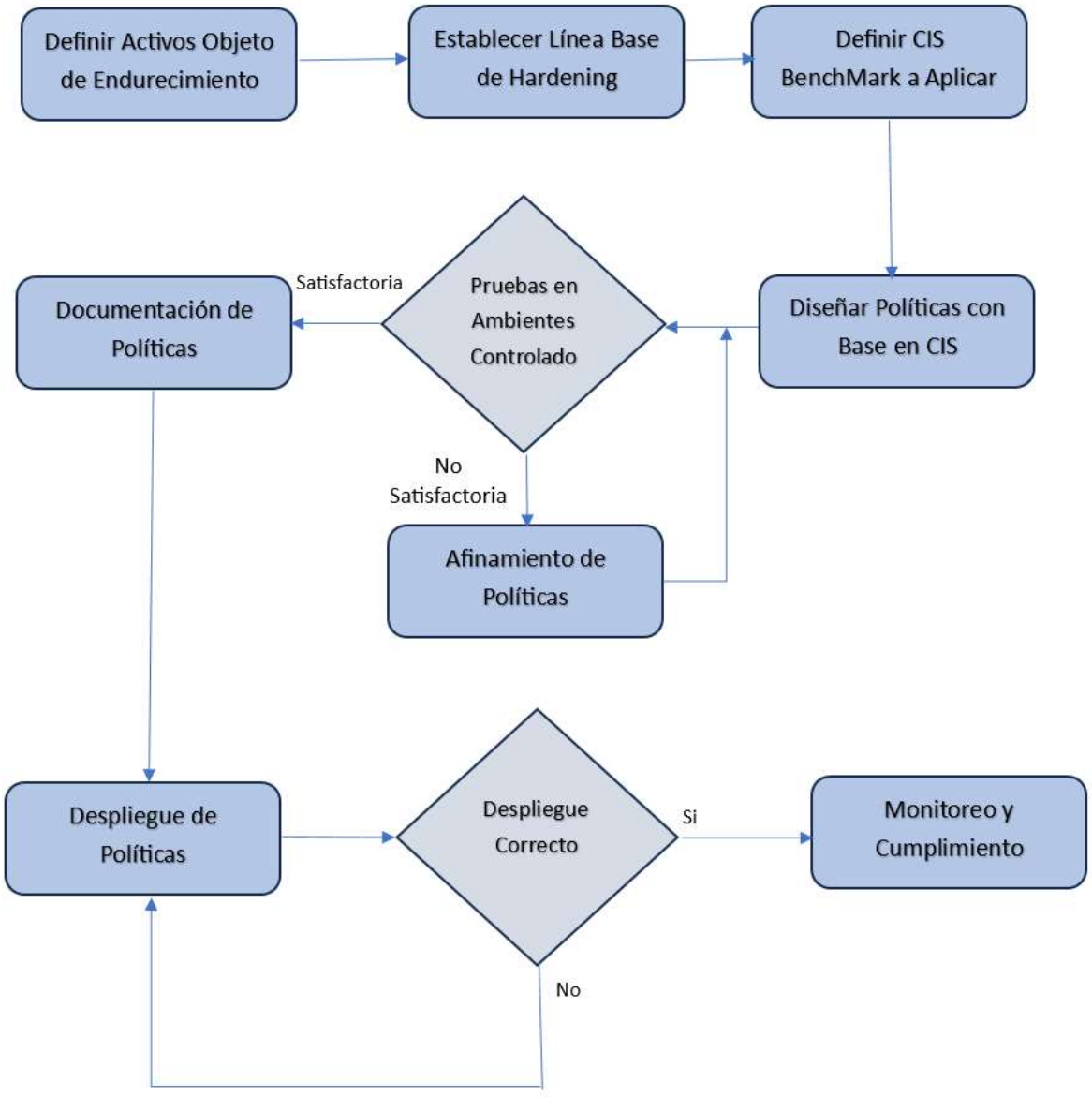
- **Herramientas de administración de configuración:** este tipo de herramientas brinda la posibilidad de realizar una administración centralizada sobre todos los componentes de una red, permiten realizar el despliegue de directivas y llevar un reporte de los elementos que se encuentran cubiertos por las políticas definidas y cuales no, la gran diferencia con las herramientas de *hardening* es que estas no están en la capacidad de realizar pruebas y medir el impacto que las directivas pueden tener sobre los ambientes de producción.

- **Herramientas de cumplimiento** Estas herramientas tienen su objetivo principal en evaluar el estado de la red respecto a un marco de cumplimiento por ejemplo CIS *benchmark*, DISA STIG entre otros, estas herramientas generan reportes que indican el estado de endurecimiento de los sistemas respecto al marco seleccionado.

Es importante tener en cuenta que el ecosistema de red es dinámico razón por la cual es necesario que el esquema de endurecimiento se encuentre en un proceso de mejora continua el cual garantice que las políticas aplicadas estén siembre acorde con los últimos lineamientos dados en este tema.

En la figura 17 se observa el flujograma del proceso de *hardening* planteado para el aseguramiento de los servidores web.

Figura 18 Diagrama Flujo Esquema de *Hardening*



Fuente: Elaboración propia

6.5.1 *Hardening* sistema operativo

Teniendo en cuenta el análisis de resultados obtenido anteriormente y con el fin de mejorar los niveles de seguridad de los servidores se propone las siguientes estrategias a implementar en el sistema operativo:

Complejidad de Contraseñas: se debe establecer políticas de seguridad de contraseñas de tal manera que estas sean robustas y no sea posible obtenerlas por

métodos tradicionales como ataques por fuerza bruta o diccionarios, para este fin se propone seguir los siguientes lineamientos:

- La longitud de las contraseñas deberá ser de 8 caracteres mínimo para usuarios que utilicen doble factor de autenticación y 14 caracteres para usuarios que no lo utilicen.

- Establecer el tiempo de vida de las contraseñas máximo 365 días o menos, en todo caso nunca se deberá usar la opción de contraseña que nunca expira, ya que entre menor sea el tiempo de vida de las contraseñas menor será la oportunidad de un atacante de violentarlas.

- Establecer parámetros de complejidad de contraseña los cuales deben validar que no se utilice partes del nombre de usuario, además contener de manera obligatoria letras mayúsculas y minúsculas, números y caracteres especiales.

- Desactivar las opciones de utilizar sistemas de encripción de contraseñas reversible, de este modo se asegura que el método de autenticación guardado en lo servidores corresponde a un Hash de la contraseña y no a la contraseña como tal, de tal forma que sea imposible obtener la contraseña a partir del Hash almacenado.

Políticas de bloqueo de cuenta es importante establecer políticas de bloqueo de cuenta por factores como intentos fallidos entre otros de esta manera se minimiza la posibilidad de que un ataque por fuerza bruta logre llegar a ser efectivo, para logar este fin se debe seguir los siguientes lineamientos:

- Establecer un tiempo de bloqueo de cuenta en 15 minutos o más, esta política hace referencia al tiempo que transcurrirá hasta que un usuario pueda intentar *logearse* nuevamente después de un bloqueo por intentos inválidos, es importante tener en cuenta que entre mayor sea el tiempo establecido mayor será la efectividad ante un ataque de fuerza bruta, sin embargo, esto puede acarrear un aumento considerable en solicitudes de soporte por motivo de desbloqueo de cuenta.

- Ajustar el bloqueo de cuenta a 5 intentos fallidos, esta política en conjunto con un tiempo elevado de bloqueo es de gran utilidad para evitar ataques de fuerza bruta.

- Establecer el tiempo de reinicio de conteo de intentos inválidos en 15 minutos, por defecto los servidores no tienen activada esta opción, si esta opción se activa el tiempo de reinicio debe ser menor o igual al tiempo de bloqueo de cuenta.

Cuentas de usuario por defecto Todos los sistemas operativos después de su instalación inicial crean ciertas cuentas de usuario por defecto, es importante darles el manejo adecuado a ellas ya que son un vector importante de ataques de parte de personas malintencionadas que quieren ganar acceso al sistema operativo

- Desactivar la cuenta Administrador por defecto, esta cuenta se crea de forma automática al momento de instalar por primera vez el sistema operativo y es una cuenta con privilegios elevados, por ende, es buena práctica deshabilitar este administrador local y crear una cuenta diferente que tenga los mismos privilegios.

- Configurar el parámetro *Block Microsoft account* con el valor *"users can´t add or log on with Microsoft accounts"* esta política se utiliza para evitar que un usuario se loguee con cuentas de usuario reservadas para el sistema operativo como el caso de la cuenta SYSTEM la cual tiene los mismos derechos que una cuenta administradora.

- Desactivar la cuenta invitado que por defecto se configura en el sistema operativo, esto por cuanto esta cuenta especial no precisa contraseña de acceso y puede ser utilizada para obtener información relevante sobre el tipo de sistema que se encuentra instalado.

Opciones de Apagado y reinicio con el fin de evitar que un sistema sea reiniciado por error o por parte de un atacante que logro acceso remoto al servidor es necesario establecer las opciones de apagado o reinicio del sistema de tal forma que no sea posible realizar estas acciones de forma remota salvo equipos remotos autorizados los cuales deberán estar debidamente identificados y en cualquier caso no deberán superar los 3 equipos autorizados para efectuar esta acción.

***Firewall* de Windows** para evitar que tráfico no deseado logre llegar hasta el sistema operativo es importante que el firewall se encuentre activado y cuente con las siguientes políticas por defecto:

- Por defecto todas las conexiones entrantes deberán ser bloqueadas, de tal forma que se pueda controlar las conexiones que serán aceptadas de forma explícita, esto brinda un mayor control sobre qué servicios y que protocolos están habilitados para conectarse al servidor.

- Todas las conexiones salientes por defecto deberán estar permitidas, de tal forma que el servidor pueda realizar las conexiones con sistemas externos que sean requeridas para su funcionamiento.

- Configurar el firewall para que no emita notificaciones en caso de que alguna conexión entrante sea bloqueada.

- Especificar el tamaño de logs de firewall en un límite no inferior a 16 Mb de tal forma que sea posible obtener un histórico del comportamiento pasado de las conexiones al servidor, para el caso de servidores con un alto tráfico de conexiones este valor deberá ser más grande o se deberá desactivar la opción de sobrescribir el archivo de logs de tal manera que siempre se tenga un log con información suficiente para el caso de algún tipo de análisis forense.

6.5.2 *Hardening* Servidor Web IIS

De otro lado es importante establecer políticas de aseguramiento sobre el servidor web, que para este caso se trata de *Internet Information services IIS* dado que este rol permitirá que peticiones realizadas desde internet sean tratadas en el servidor y por este motivo los vectores de ataque serán mayores, por esta razón es importante seguir los siguientes lineamientos que tienen como objetivo asegurar el servidor web

Configuración Básica al momento de realizar la instalación de la característica de servidor web, esta instalación toma configuraciones por defecto las cuales son conocidas por los atacantes y de no darles el tratamiento adecuado podrían dar paso a incidentes de seguridad que pondrán en juego la estabilidad de los portales web o la información ahí contenida.

- Es importante que todo el contenido web, se encuentre en una partición diferente a la que se encuentra el sistema de esta manera se minimiza el área afectada en caso de que un ataque sea efectivo, esta característica es útil en casos en los que existe más de un portal o aplicación web alojada en el mismo servidor, puesto que un ataque efectivo afectaría solo a un portal, en caso de no aplicar esta configuración un ataque podría llegar a afectar el sistema operativo y por consiguiente todos los portales o aplicaciones web alojadas.

- Configurar "*Host Headers"* en todos los sitios alojados, de esta manera será posible mantener varios sitios web con una única dirección ip y reducir la probabilidad de escaneos basados en direcciones ip.

- Desactivar la opción de exploración de directorio, cuando esta opción se encuentra activada el contenido de un directorio puede ser desplegado en un explorador permitiendo a un atacante tener acceso a código fuente de la aplicación, archivos de configuración entre otros, esta información puede ser utilizada con posterioridad para orquestar ataques más definidos.

Recomendaciones respecto a Logs de eventos Los logs de eventos son archivos que contienen información importante sobre el comportamiento de la aplicación y las interacciones que esta ha tenido con los usuarios externos, también en estos archivos se puede encontrar información importante sobre cómo se efectuó un

ataque o que recursos se vieron afectados, es por este motivo que es importante asegurar esta información.

- Cambiar la ruta por defecto en la cual se almacenan los archivos de log, es importante ya que estos archivos son lo primero que hay que asegurar en caso de un incidente de seguridad.

- Activar la toma de logs avanzada, esta característica permite que la información almacenada en los archivos pueda ser personalizada de acuerdo con las necesidades de cada grupo de seguridad estableciendo que campos son importantes cuales no, además de posibilitar tener campos adicionales a los que por defecto se almacenan.

- Activar la nueva característica de *loggin* denominado *ETW Logging* que permite que los logs sean enviados al servicio *Event Tracing for Windows (EWT).*

Encriptación en transporte es importante que el tráfico entre la aplicación web y el usuario final se realice de forma segura esto implica que todo el tráfico debe estar encriptado y utilizando protocolos que no sean fácilmente vulnerables, para lograr este objetivo se debe:

- Activar el encabezado HSTS, esto permite que el sitio informe al usuario que la comunicación se realizará únicamente sobre el protocolo HTTPS, de esta manera se asegura que los visitantes al sitio hagan uso únicamente de protocolo seguro y transporte cifrado.

- Desactivar protocolos débiles por ejemplo se debe desactivar los protocolos SSLv2 y SSLv3 puesto que estos se consideran criptográficamente inseguro.

- Desactivar el protocolo TLS 1.1 este protocolo se considera débil y se utilizó hace algún tiempo para dar compatibilidad a aplicaciones antiguas en la actualidad se debe desactivar salvo casos específicos en los cuales sea requerido.

- Activar el protocolo TLS 1.2 puesto que este es el protocolo más reciente y se encuentra en un alto grado de madurez brindando confidencialidad e integridad al tráfico HTTP

6.5.3 *Hardening* Conexiones Remotas RDP

Teniendo en cuenta que en los servidores analizados se evidencia que existen conexiones remotas mediante protocolo RDP es fundamental aplicar políticas de *hardening* sobre este tipo de conexiones debido a que este protocolo es conocido por ser uno de los principales objetivos al momento de ser víctima de un ataque informático

- No permitir Guardar la contraseña o cuenta de usuario en el cliente RDP, se debe desactivar esta opción puesto que un atacante que logre tener acceso físico a un equipo desde donde se generen conexiones remotas fácilmente puede obtener acceso a los servidores sin la necesidad de conocer las credenciales de acceso ya que estas se encuentran guardadas en el cliente de conexión remota.

- Activar la política *'Restrict Remote Desktop Services users to a single Remote Desktop Services session'* mediante la activación de esta política se asegura que un usuario que realiza conexiones remotas sobre el servidor siempre utilice la misma sesión, de esta manera en caso de una desconexión cuando el usuario se reconecte ingresara a la sesión que ya se encontraba creada de esta forma se evita que un usuario logre tener sesiones activas paralelas de la misma forma se optimiza el uso de recursos de hardware.

- Evitar el redireccionamiento de *drives:* Los datos se pueden reenviar desde la sesión de Servicios de Escritorio remoto del usuario a la sesión del usuario equipo local. En este caso un software malintencionado ya presente en un equipo remoto comprometido tendría acceso directo y sigiloso al disco local del servidor durante la sesión de escritorio remoto, logrando afectar los datos contenidos en el servidor.

- Activar la opción *'Always prompt for password upon connection'* , es importante activar la opción de que siempre que se requiera establecer una conexión remota se solicite las credenciales de acceso, de tal forma que se minimice la posibilidad de que un atacante que logró acceder a un equipo de usuario logre saltar a un servidor remoto.

- El servidor únicamente debe recibir conexiones remotas de clientes que utilicen conexiones seguras, de esta forma se evita que el servidor quede expuesto a ataques de hombre en el medio evitando conexiones desde clientes RDP en los cuales no se confía.

- Establecer en la configuración de las conexiones remotas que se requiera de un nivel de cifrado específico durante el proceso de conexión de esta manera se evita que el tráfico entre los participantes de la conexión pueda ser interceptado y modificado.

- Establecer un tiempo límite para inactividad en conexiones remotas, de esta manera se puede establecer un tiempo límite durante el cual una sesión puede estar abierta y sin actividad transcurrido este tiempo la sesión se debe cerrar de tal manera que el usuario al reconectarse deba nuevamente proporcionar sus credenciales, esto con el fin de evitar que terceras personas logren ingresar de forma remota al servidor ante un descuido del usuario autorizado.

6.5.4 *Hardening* Base de Datos

- Con el fin de minimizar la posibilidad de una denegación de servicios sobre el motor de base de datos es recomendable que los archivos que contienen las distintas bases de datos se encuentren almacenados en particiones o sistemas de archivos diferentes a los del sistema operativo, de esta manera también se evita que la base de datos se vea afectada por temas como agotamiento de espacio disponible.

- Utilizar cuentas de servicio con el mínimo de privilegios para ejecutar lo servicios del motor de base de datos, de esta manera es posible que los servicios se ejecuten dentro de un contexto de usuario restringido minimizando de esta forma la posibilidad de que una vulnerabilidad sea explotada y ponga en riesgo el sistema operativo del servidor.

- Evitar que el motor de base de datos pueda obtener credenciales desde la variable de entorno *MYSQL_PWD* evitar el uso de esta variable establece un nivel mucho más alto de confidencialidad de las contraseñas que utiliza el motor.

- Verificar que existan políticas de respaldo sobre las bases de datos y que estos respaldos se encuentren cifrados de tal forma que si por algún motivo uno de estos backups es interceptado por un atacante sea imposible para este obtener el contenido.

- El motor de base de datos debe correr en un servidor dedicado de tal manera que el acceso a este de parte de usuario y aplicaciones sea mínimo y esté totalmente controlado de esta forma se reduce sustancialmente el área de ataque.

- No reutilizar nombres de usuario en varias aplicaciones, el uso de cuentas de usuario independientes para conexiones de aplicaciones con el motor de base de datos reduce el impacto que se podría producir en caso de que una cuenta se vea comprometida ya que cada base de datos almacenada en el servidor estará separada y su acceso será mediante diferentes credenciales.

- Establecer políticas de cambio de contraseña y complejidad de esta de tal forma que los usuarios se vean obligados a cambiar su contraseña cada determinado periodo de tiempo, esto es una salvaguarda de gran utilidad en contra de ataques por diccionario o fuerza bruta.

6.5.5 *Hardening* protocolo FTP

El protocolo de transferencia de archivos es ampliamente utilizado en los servidores web con diferentes objetivos y brinda una potente herramienta para el manejo de código fuente o archivos por parte de los usuarios finales, sin embargo, si este protocolo no se asegura de forma adecuada implica un alto riesgo para la

confidencialidad y seguridad de la información, por este motivo se deben tener en cuenta las siguientes recomendaciones:

- Todas las solicitudes FTP deberán estar encriptadas, el servicio FTP de IIS soporta el uso de certificados SSL en un sitio FTP, el utilizar estos certificados se conoce con el nombre de SFTP o FTP sobre SSL, el uso de esta técnica garantiza que la transmisión de datos entre el servidor y el cliente sea encriptada incluyendo las credenciales de conexión.

- Activar la nueva característica que introduce IIS denominada *FTP Logon attempt restrictions*, esta nueva característica bloquea automáticamente los ataques por fuerza bruta.

- Establecer políticas de complejidad sobre las contraseñas de acceso de tal manera que se dificulte o imposibilite un ataque por fuerza bruta o diccionario.

- Restringir el acceso a carpetas determinadas por ningún motivo se debe permitir que un usuario tenga acceso a todo un volumen o disco, cada usuario debe tener acceso a carpetas independientes.

7 CONCLUSIONES

Las herramientas utilizadas para el análisis son herramientas de fácil manejo y comprensión sin dejar de ser potentes en la identificación de debilidades presentes que a simple vista pueden pasar desapercibidas y se convierten en un riesgo latente que puede poner en riesgo la operación de los servicios

La realización de análisis tipo *pentesting* sobre los servidores web se debe convertir en una tarea recurrente debido a que el constante avance de la tecnología lleva a descubrir cada día nuevas amenazas y vulnerabilidades que deben ser eliminadas o en caso de no ser posible su eliminación mitigar su impacto.

Los análisis realizados sobre los servidores objeto de estudio arrojaron un gran número de vulnerabilidades las cuales pueden ser explotadas por un atacante logrando impactar la información contenida en los portales web de la entidad, se evidencia que la gran mayoría de debilidades corresponden a versiones obsoletas del *framework* PHP y en un menor porcentaje vulnerabilidades asociadas a sistema operativo y aplicaciones web.

El aseguramiento de los servidores web se debe enfocar desde dos aspectos principales, el primero aplicar las recomendaciones de *hardening*, que tienen como objetivo evitar que personas no autorizadas logren acceso al sistema operativo y por ende puedan efectuar actividades de robo de información o denegación de servicios de alto impacto, el segundo es aplicar las salvaguardas asociadas a las vulnerabilidades del sistema operativo del servidor actividad que brindará a la Unidad Administrativa Especial de Servicios Públicos la posibilidad de mantener la información segura y libre de posibles ataques externos que podrían llegar a ser de alto impacto dada la naturaleza de la entidad.

8 RECOMENDACIONES

Teniendo en cuenta la situación actual de la Unidad Administrativa Especial de Servicios Públicos de Bogotá y los resultados obtenidos en el presente proyecto se puede evidenciar que existe una gran cantidad de debilidades asociadas a los servidores web por lo que es necesario que se establezcan planes de trabajo enfocados en la mitigación o eliminación de dichas debilidades los cuales se recomienda estén enfocados en dos aspectos fundamentales:

El primero en atacar las falencias que están presentes a nivel de aplicaciones web para lo cual se recomienda realizar la actualización del *framework* PHP a una versión más reciente, esta actualización disminuirá en gran medida la cantidad de vulnerabilidades detectadas en los servidores web de la Entidad; también es importante que se diseñen planes de escaneo de vulnerabilidades periódicos de tal forma que el área de tecnología cuente siempre con información actualizada sobre el estado de seguridad de sus servidores y en caso de aplicar alguna actualización necesaria esta se realice de forma escalonada disminuyendo el posible impacto que esta podría tener sobre los ambientes de producción.

Como un segundo aspecto se debe aplicar las recomendaciones de *hardening* que tienen como objetivo principal evitar que usuarios no autorizados logren tener acceso al sistema operativo del servidor y por consiguiente tener control total de las aplicaciones web, este punto es de suma importancia ya que dada la naturaleza de la entidad un ataque de denegación de servicios realizado desde el interior tendría un impacto sumamente alto en la operación del servicio y por ende en la ciudadanía de Bogotá.

Por la razón anteriormente descrita es importante basarse en guías y buenas prácticas para los procesos de *hardening* de servidores las cuales nos dan lineamientos de aseguramiento que han sido evaluados por expertos en el tema y que tienen un elevado nivel de impacto en el aseguramiento de estos activos de información, basado en lo anterior se recomienda acogerse a las buenas prácticas establecidas por el CIS *Center for Internet security* específicamente las contenidas en "*CIS Benchmarks for Microsoft Windows Server 2012 R2*" en su última versión, la aplicación de estos lineamientos en conjunto con la instalación de parches de seguridad lograran que los niveles de seguridad de los servidores se vean elevados de forma considerable.

Por otro lado es necesario mencionar que las recomendaciones anteriores están enfocadas en temas confidencialidad e integridad de la información sin embargo no se debe dejar a un lado los temas relacionado scon la disponibilidad de los servicios por lo cual es importante mencionar que la organización debe establecer planes de respaldo de la información estos planes de respaldo deben considerar el almacenamiento de copias de respaldo en varias ubicaciones un repositorio local y

uno geográficamente separado, en la actualidad se recomienda el uso de servicios de nube publica para el almacenamiento de estas copias de seguridad ya que estos servicios brindan niveles elevados de capacidad de almacenamiento como de aseguramiento y su escalabilidad está asegurada.

También es importante sugerir que dada la naturaleza de la entidad la disponibilidad de sus servicios debe estar garantizada por lo cual adicional a las copias de respaldo se sugiere la implementación de esquemas de recuperación ante desastres o DRP (*Disaster Recovery Plan*), estos esquemas garantizarán que la operación de los servicios críticos de la organización no se vean afectados por situaciones externas de difícil control como por ejemplo un asonada o desastre natural, la implementación de este tipo de esquemas logrará que la organización llegue a un nivel alto en temas de disponibilidad ya que sus servicios e información estarán siempre disponibles y su operación no se verá afectada.

9 DIVULGACIÓN

El desarrollo del presente proyecto de grado será dado a conocer en colaboración de la biblioteca de la Universidad Nacional Abierta y a Distancia – UNAD, a través de su aplicativo en línea, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este; con el fin de que todos los estudiantes de la Universidad que se encuentren interesados en el tema de Diseño de un esquema de hardening para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá, puedan acceder al documento.

BIBLIOGRAFÍA

ACOSTA, David E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST [blog]. David E. Acosta Blog personal. Barcelona, España. 11 de junio de 2017. [Consultado: 20 de febrero de 2023]. Disponible en: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/

ALTUBE VERA, Rafael. Qué es OpenVAS [blog]. Openwebinars. 11 de noviembre de 2020. [Consultado: 14 de diciembre de 2022]. Disponible en: https://openwebinars.net/blog/que-es-openvas/

ÁLVAREZ HUERTA, Leopoldo. OpenVas en Linux: Explorando nuestros sistemas [blog]. Openwebinars. 30 de mayo de 2014. [Consultado: 14 de diciembre de 2022]. Disponible en: https://openwebinars.net/blog/openvas-en-linux-explorando-nuestros-sistemas/

ASENCIO MENDOSA, Martha y MORENO PATIÑO, Pedro Julián. Desarrollo de una propuesta Metodológica para Determinar la Seguridad en una Aplicación. Trabajo de investigación Ingeniero de Sistemas y Computación. Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería Sistemas y Computación. 2011. 79 p. [Consultado: 10 de diciembre de 2022]. Disponible en: https://repositorio.utp.edu.co/server/api/core/bitstreams/f4d085e0-d12b-49f8-80aa-ea62228b18b6/content

BECOLVE DIGITAL. ¿Qué es un firewall industrial DPI (Deep Packet Inspection)? [blog]. CIBERSEGURIDAD. 18 de septiembre de 2014. [Consultado: 6 de marzo de 2023]. Disponible en: https://www.ciberseguridadlogitek.com/que-es-un-firewall-industrial-dpi-deep-packet-inspection/

CABALLERO QUEZADA, Alonso Eduardo. ZAP. OWASP Zed Attack Proxy [Webinar]. mayo de 2016. [Consultado: 12 de noviembre de 2023]. Disponible en: https://www.slideshare.net/reydes/webinar-owasp-zed-attack-proxy-zap

CAMPUS CIBERSEGURIDAD - ENIIT INNOVA BUSINESS SCHOOL. ¿Qué es el Pentesting? [blog]. Valladolid, España. 16 de noviembre de 2022. [Consultado: 2 de octubre de 2022]. Disponible en: https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting

CASTRO, Jandro. UN CATÁLOGO DE SERVICIOS NO ES UNA LISTA DE APLICACIONES [blog]. Proactivanet. 28 de enero de 2014. [Consultado: 30 de noviembre de 2023]. Disponible en: https://www.proactivanet.com/blog/catalogo-de-servicios/un-catalogo-de-servicios-no-es-una-lista-de-aplicaciones/

CISET, Centro de Innovación. Hardening [blog]. Leganés, Madrid España. 4 de octubre de 2020. [Consultado: 10 de marzo de 2023]. Disponible en: https://www.ciset.es/publicaciones/blog/746-hardening

COMPILAR NEWS. Comandos Nmap con ejemplos [blog]. 1 de marzo de 2021. [Consultado: 8 de abril de 2023]. Disponible en: https://conpilar.es/comandos-nmap-con-ejemplos/

COORDINACIÓN TIC. La tecnología y su impacto en la auditoría interna de las organizaciones [blog]. INCP. Colombia. 16 agosto de 2019. [Consultado: 8 de marzo de 2023]. Disponible en: https://incp.org.co/la-tecnologia-impacto-la-auditoria-interna-las-organizaciones/

DOCUSING. Disponibilidad de la información: ¿Por qué es importante contar con opciones seguras? [blog]. 17 de agosto de 2021. [Consultado: 13 de enero de 2023]. Disponible en: https://www.docusign.mx/blog/disponibilidad-de-la-informacion

ECHEVERRÍA USÚA, Javier. Hacking ético: identificación de servicios con nmap [en línea]. VIAFIRMA. 14 de octubre de 2019. [Consultado: 3 de marzo de 2023]. Disponible en: https://www.viafirma.com/blog-xnoccio/es/identificacion-servicios-nmap/

ECURED. Ataques Informáticos [blog]. 18 de julio de 2019. [Consultado: 7 de marzo de 2023]. Disponible en: https://www.ecured.cu/Ataque_inform%C3%A1tico

EQUIPO DE EXPERTOS DE CIENCIA Y TECNOLOGÍA DE LA UNIVERSIDAD INTERNACIONAL DE VALENCIA. ¿Qué es la seguridad informática y cómo puede ayudarme? [sitio web]. Universidad Internacional de Valencia. 9 de septiembre de 2016. [Consultado: 11 de diciembre de 2022]. Disponible en: https://www.universidadviu.com/co/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme

EUROPEAN KNOWLEDGE CENTER FOR INFORMATION TECHNOLOGY. Servidores [blog]. TIC Portal. 8 de julio de 2019. [Consultado: 1 de febrero de 2023]. Disponible en: https://www.ticportal.es/glosario-tic/servidores

GARCIA, Noelia. Clasificación y tipos de ataques contra sistemas de información [en línea]. vLex. [Consultado: 7 de febrero de 2023]. Disponible en: https://vlex.es/vid/clasificacion-tipos-ataques-sistemas-102081

GENEZ, Gustavo. OWASP ZAP, audita la seguridad de webs y evita vulnerabilidades [blog]. Seguridad PY. 6 de mayo de 2021. [Consultado: 20 de marzo de 2023]. Disponible en: https://seguridadpy.info/2021/05/owasp-zap-audita-la-seguridad-de-webs-y-evita-vulnerabilidades/

HACKNOID. Importancia de la seguridad informática de las empresas [blog]. Uruguay. 2 de julio de 2019. [Consultado: 18 de enero de 2023]. Disponible en: https://www.hacknoid.com/hacknoid/importancia-de-la-seguridad-informatica-de-las-empresas/

INCIBE. Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? [blog]. Instituto de Ciberseguridad. España. 20 de marzo 2017. [Consultado: 12 de enero de 2023]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian#:~:text=Una%20vulnerabilidad%20(en%20t%C3%A9rminos%20de,necesario%20encontrarlas%20y%20eliminarlas%20lo

INISEG. ¿Qué es el Hacking ético? Concepto y formación profesional [blog]. Ciberseguridad. Getafe, Madrid España. 6 de agosto de 2018. [Consultado: 26 de febrero de 2023]. Disponible en: https://www.iniseg.es/blog/ciberseguridad/que-es-el-hacking-etico/

INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN - ICONTEC. Sistemas de gestión de la seguridad de la Información: Técnicas de seguridad y requisitos. NTC-ISO/IEC 27001 [en línea]. Bogotá D.C.: El Instituto, 2013. 45 p. [Consultado: 30 de noviembre de 2022]. Disponible en: https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf

INSTITUTO NACIONAL DE TECNOLOGÍAS EDUCATIVAS Y DE FORMACIÓN DEL PROFESORADO (INTEF). Seguridad Informática. Elementos vulnerables en el sistema informático [sitio web]. Madrid, España. [Consultado: 30 de diciembre de 2022]. Disponible en: http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/elementos_vulnerables_en_el_sistema_informtico.html

ISOTOOLS EXCELLENCE. ¿Qué es la seguridad de la información y cuantos tipos hay? [blog]. PMG SSI. 11 de marzo de 2021. [Consultado: 23 de abril de 2023]. Disponible en: https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

MENDOZA, Miguel Ángel. Cómo utilizar OpenVAS para la evaluación de vulnerabilidades [blog]. Welivesecurity. 18 de noviembre de 2014. [Consultado: 14 de febrero de 2023]. Disponible en: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

MILLAN TEJEDOR, Ramón Jesús. Que es SNMP V3 (Simple Network Management Protocol versión 3) [en línea]. Consultoría estratégica en tecnologías de la información y comunicaciones. [Consultado: 1 de febrero de 2023]. Disponible en: https://www.ramonmillan.com/tutoriales/snmpv3.php

NMAP.ORG. [sitio web]. [Consultado: 13 de febrero de 2023]. Disponible en: https://nmap.org/

OPENIT. ¿Qué es el hardening de sistemas operativos? [blog]. Argentina. [Consultado: 13 de marzo de 2023]. Disponible en: https://www.openit.com.ar/que-es-el-hardening-de-sistemas-operativos/

ORACLE. Referencia de gestión de protocolos para SNMP e IPMI de Oracle® ILOM, versión de firmware 3.2.x. Componentes de SNMP [sitio web]. [Consultado: 10 de marzo de 2023]. Disponible en: https://docs.oracle.com/cd/E40701_01/html/E40347/z4002eb91391913.html

OTEGUI GARCÍA, Alejandro. Herramientas de análisis de vulnerabilidades [Webinar]. 20 de octubre de 2017. [Consultado: 27 de enero de 2023]. Disponible en: https://es.slideshare.net/alejandro_otegui96/herramientas-de-anlisis-de-vulnerabilidades-81021908

OWASP. Welcome to the OWASP Top 10 - 2021 [sitio web]. [Consultado: 24 de febrero de 2023]. Disponible en: https://owasp.org/Top10/

PARDO LORENZO, Andrea María. TEMA 4: SEGURIDAD INFORMÁTICA. 4) ATAQUES A LOS SISTEMAS INFORMÁTICOS. 4.1) TIPOS DE ATAQUES [blog]. Blog de Seguridad. 13 de noviembre de 2016. [Consultado: 10 de enero de 2023]. Disponible en: https://blogseguridadandrea.wordpress.com/2016/11/13/4-1-tipos-de-ataques/

PICO, Pablo. Tipos de ataque informático [blog]. El blog del ingeniero de sistemas. Colombia. [Consultado: 14 de abril de 2023]. Disponible en: https://ingenierodesistemas.co/informatica/tipos-ataques-informatico/

SEGUIDORES ONLINE. Los Puertos de Comunicación y Sus Funciones [sitio web]. [Consultado: 3 de enero de 2023]. Disponible en: https://intelectouniversal.com/comunicaciones/puertos-de-comunicacion/

SEGUNDO ESPÍNOLA, Juan Pablo. Método deductivo [blog]. Concepto de. Argentina. 29 de julio de 2022. [Consultado: 12 de marzo de 2023]. Disponible en: https://concepto.de/metodo-deductivo/

SENSAGENT - DICCIONARIO. Puerto de red En: diccionario.sensagent.com/ [Consultado: 14 de enero de 2023]. Disponible en: http://diccionario.sensagent.com/puerto%20de%20red/es-es/

SNIFER@L4B'S. Listado Completo Herramientas en Kali Linux [sitio web]. 23 de marzo de 2014. [Consultado: 4 de noviembre de 2022]. Disponible en: https://sniferl4bs.com/2014/03/listado-completo-herramientas-en-kali-linux/

TERRAETICA. Levantamiento de información cualitativa y cuantitativa [sitio web]. Cátedra de Medición de impacto 2020-21. México. [Consultado: 29 de enero de 2023]. Disponible en: https://terraetica.com/levantamiento-de-informacion-cualitativa-y-cuantitativa

UCHA, Florencia. Definición de Confidencialidad En: DEFINICIONABC.com. Agosto de 2010. [Consultado: 16 de enero de 2023]. Disponible en: https://www.definicionabc.com/comunicacion/confidencialidad.php

VELÁZQUEZ, M. Cornejo, et al. Principios de Seguridad Informática en Sistemas de Información. XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan, 2015, vol. 3, no 6. [Consultado: 12 de diciembre de 2022]. Disponible en: https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n6/e5.html

WAGNER, Jarvis. ¿Cómo hacer análisis de vulnerabilidades informáticas? [en línea]. 2 de marzo de 2016. [Consultado: 3 de abril de 2023]. Disponible en: https://noticiasseguridad.com/tecnologia/como-hacer-analisis-de-vulnerabilidades-informaticas/

WEST, Darrell M. Avance tecnológico: riesgos y desafíos. En: *Openmind BBVA.* [Consultado: 14 de febrero de 2023]. Disponible en: https://www.bbvaopenmind.com/articulos/avance-tecnologico-riesgos-y-desafios/

Anexo 1.

RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Tema	Diseño de un esquema de Hardening, basado en los resultados obtenidos de pruebas de vulnerabilidad realizado sobre servidores web de la Unidad Administrativa Especial de Servicios Públicos de Bogotá
Titulo	Diseño de un esquema de hardening para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá
Autor(es)	Oscar Ricardo Rodríguez Martínez
Director	Magister Gestión en Tecnologías de la Información, Ingeniero Hernando José Peña Hidalgo
Fuente Bibliográfica	Se referencia 42 fuentes bibliográficas, algunas que mencionan la temática principal son: ACOSTA, David E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST [blog]. David E. Acosta Blog personal. Barcelona, España. 11 de junio de 2017. [Consultado: 20 de febrero de 2023]. Disponible en: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/ ASENCIO MENDOSA, Martha y MORENO PATIÑO, Pedro Julián. Desarrollo de una propuesta Metodológica para Determinar la Seguridad en una Aplicación. Trabajo de investigación Ingeniero de Sistemas y Computación. Universidad Tecnológica de Pereira. Facultad de Ingenierías. Programa de Ingeniería Sistemas y Computación. 2011. 79 p. [Consultado: 10 de diciembre de 2022]. Disponible en: https://repositorio.utp.edu.co/server/api/core/bitstreams/f4d085e0-d12b-49f8-80aa-ea62228b18b6/content CABALLERO QUEZADA, Alonso Eduardo. ZAP. OWASP Zed Attack Proxy [Webinar]. mayo de 2016. [Consultado: 12 de noviembre de 2023]. Disponible en: https://www.slideshare.net/reydes/webinar-owasp-zed-attack-proxy-zap INSTITUTO COLOMBIANO DE NORMALIZACIÓN Y CERTIFICACIÓN - ICONTEC. Sistemas de gestión de la seguridad de la Información: Técnicas de seguridad y requisitos. NTC-ISO/IEC 27001 [en línea]. Bogotá D.C.: El Instituto, 2013. 45 p. [Consultado: 30 de noviembre de 2022]. Disponible en: https://serviciocivil.gov.co/sites/default/files/marco-legal/2006_03_22_NTC-ISO-IEC%2027001.pdf VELÁZQUEZ, M. Cornejo, et al. Principios de Seguridad Informática en Sistemas de Información. XIKUA Boletín Científico de la Escuela Superior de Tlahuelilpan, 2015, vol. 3, no 6. [Consultado: 12 de diciembre de 2022]. Disponible en: https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n6/e5.html
Año	2023

Resumen	Actualmente el mundo se encuentra inmerso en un proceso de rápidos cambios y avances en temas de tecnología, estos tienen como función principal cubrir necesidades, facilitar tareas rutinarias o hacer que la información sea de carácter masivo y de acceso fácil para todas las personas. Así la información se convierte en uno de los activos más importante en cualquier compañía, no obstante, el rápido crecimiento tecnológico ha generado diferentes riesgos que pueden ser aprovechados por personas mal intencionadas. Lo anterior, ha llevado a que las instituciones requieran establecer métodos y lineamientos que permitan salvaguardarla y al tiempo mantener los tres pilares de la seguridad de la información que son integridad, confidencialidad y disponibilidad. En este contexto cobra importancia dentro las organizaciones procesos como la hardenización cuyo propósito es el fortalecimiento del sistema informático que minimice las vulnerabilidades de seguridad de la información y aumente la protección del sistema contra posibles amenazas. Dentro de estas organizaciones se encuentra la Unidad Administrativa Especial de Servicios Públicos entidad que maneja información oficial y que dentro de su renovación de infraestructura tecnológica se ha visto vulnerable a posibles riesgos en la seguridad. Por ello el objetivo de este trabajo fue diseñar un esquema de hardening para los servidores web de la oficina TIC de esta entidad pública de Bogotá.
Palabras Claves	Hardening, Salvaguardas, Seguridad Informática, Vulnerabilidades
Contenidos	

	b. Inventario de aplicaciones c. Pruebas de comportamiento de herramientas y análisis de vulnerabilidades d. Verificación de puertos e. Análisis de vulnerabilidades f. Análisis de aplicaciones web 14. ANALISIS DE RESULTADOS a. Escaneo de puertos b. Escaneo de Vulnerabilidades c. Escaneo Aplicación web d. Estrategias de Hardening e. Hardening sistema operativo f. Hardening Servidor Web IIS 15. CONCLUSIONES 16. RECOMENDACIONES 17. DIVULGACIÓN 18. BIBLIOGRAFÍA

3. Objetivos
OBJETIVO GENERAL Diseñar un esquema de *hardening* para los servidores web de la oficina TIC de la Unidad Administrativa Especial de Servicios Públicos de la ciudad de Bogotá a partir de un análisis de vulnerabilidades que mejore los niveles de seguridad. OBJETIVOS ESPECÍFICOS • Evaluar herramientas para el análisis de vulnerabilidades en servidores web mediante un análisis comparativo para su aplicación en la infraestructura tecnológica. • Probar herramientas para la auditoria de servidores web mediante ejercicios de *pentesting* para la identificación de vulnerabilidades. • Analizar los resultados de las pruebas de seguridad aplicadas a los servidores web mediante una revisión de los informes técnicos para el establecimiento de salvaguardas necesarias. • Proponer estrategias de *hardening* para la infraestructura de servidores basado en marcos de buenas prácticas que permita mejorar la seguridad digital.

2. Descripción del problema de investigación

La Unidad Administrativa Especial de Servicios Públicos maneja información oficial sobre temas de recolección de basuras en la ciudad de Bogotá, para este fin la entidad ha venido adelantando procesos de renovación tecnológica que la lleven a estar a la vanguardia en cuanto a la disponibilidad de sus servicios, esta evolución en temas de infraestructura tecnológica da pie a posibles riesgos o nuevas amenazas.

Es importante destacar que las vulnerabilidades se pueden presentar en dos ámbitos: mediante acceso físico a los servidores o mediante acceso informático, siendo este el más importante ya que es el más difícil de controlar.

Por otro lado, la institución presenta una alta rotación de personal, en el año 2021 el 70% del talento humano de la oficina TIC se vinculó en los últimos 6 meses, lo que conlleva a que el estado de seguridad de los servidores no sea conocido al detalle generando un alto riesgo sobre la información contenida en ellos.

4. Metodología

En el presente proyecto se utilizara un método de investigación deductivo el cual inicia desde lo general hacia lo particular para lograr un entendimiento general de los componentes de la infraestructura tecnológica de la organización y de esta manera poder proceder a realizar una búsqueda de debilidades o fallas que representen un riesgo para la información con esta información será posible plantear un plan de trabajo encaminado a endurecer las políticas de seguridad y de esta manera minimizar el riesgo de robo o daño a los datos sensibles de la entidad.

Para dar cumplimiento a los objetivos del proyecto se realizarán las siguientes actividades:

Levantamiento de información: la forma en la que se levanta la información puede potenciar o retrasar la metodología utilizada para el desarrollo de un proyecto

Enumeración de servicios y aplicaciones una vez identificada la infraestructura fisca es necesario realizar un inventario detallado de los distintos sistemas de información o aplicaciones en los ambientes web de producción y pruebas, es fundamental asociar este inventario de aplicaciones con el inventario de hardware obtenido en el proceso de levantamiento de información a fin de determinar si existe la posibilidad que un solo servidor este alojando más de una aplicación.

Identificación de herramientas a utilizar con la información recolectada y con un conocimiento claro de los servidores que hacen parte de los ambientes de pruebas y producción se procederá a identificar las herramientas adecuadas para realizar el análisis de vulnerabilidades, para este fin se tomara como base la suite KALI LINUX, la cual contienen un compilado de numerosas herramientas de detección y análisis

5. Referentes teóricos

Se realiza consulta de diferentes fuentes y se enfoca en la descripción de temas relacionados con diseño de esquemas de hardening, y pruebas de vulnerabilidades en servidores.

6. Referentes conceptuales

Se reseña diferentes conocimientos que ayudan a un adecuado análisis y comprensión de pruebas de escaño de vulnerabilidades y esquemas de aseguramiento en servidores y aplicaciones web, entre los que se encuentra: la arquitectura de servidores web de la Unidad Administrativa de Servicios Públicos de la ciudad de Bogotá.

7. Resultados

- Listado de vulnerabilidades detectadas en los servidores web
- Listado de vulnerabilidades web detectadas en el portal de la entidad
- Matriz de vulnerabilidades y salvaguardas necesarias para aseguramiento de la infraestructura que soporta los portales web de la entidad
- Recomendaciones de buenas prácticas a implementar en los servidores web con el fin de mejorar los niveles de seguridad.

8. Conclusiones

Las herramientas utilizadas para el análisis son herramientas de fácil manejo y comprensión sin dejar de ser potentes en la identificación de debilidades presentes que a simple vista pueden pasar desapercibidas y se convierten en un riesgo latente que puede poner en riesgo la operación de los servicios

Los análisis realizados sobre los servidores objeto de estudio arrojaron un gran número de vulnerabilidades las cuales pueden ser explotadas por un atacante logrando impactar la información contenida en los portales web de la entidad, se evidencia que la gran mayoría de debilidades corresponden a versiones obsoletas del framework PHP y en un menor porcentaje vulnerabilidades asociadas a sistema operativo y aplicaciones web.

El aplicar las recomendaciones de hardening, así como las salvaguardas asociadas a las vulnerabilidades del sistema operativo del servidor brindará a la Unidad Administrativa Especial de Servicios Públicos la posibilidad de mantener la información segura y libre de posibles ataques externos que podrían llegar a ser de alto impacto dada la naturaleza de la entidad.