ANÁLISIS DE RIESGO SOBRE EL SISTEMA DE SEGURIDAD INFORMÁTICA DE UNA ENTIDAD ESTATAL COMO CASO DE ANÁLISIS SIMULADO EN UN AMBIENTE CONTROLADO

WILLIAM ENRIQUE SALCEDO RODRÍGUEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ - TOLIMA

NOVIEMBRE 2020

ANÁLISIS DE RIESGO SOBRE EL SISTEMA DE SEGURIDAD INFORMÁTICA DE UNA ENTIDAD ESTATAL COMO CASO DE ANÁLISIS SIMULADO EN UN AMBIENTE CONTROLADO

WILLIAM ENRIQUE SALCEDO RODRÍGUEZ

PROYECTO DE GRADO

PRESENTADO COMO REQUISITO PARA OPTAR POR EL TÍTULO DE ESPECIALISTA EN SEGURIDAD INFORMÁTICA

DIRECTOR:

EDGAR ROBERTO DULCE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

IBAGUÉ - TOLIMA

NOVIEMBRE 2020

NOTA DE ACEPTACIÓN

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

Ibagué Tolima, Noviembre 2020

DEDICATORIA

A Dios.

Por darme las fuerzas necesarias para poder llegar hasta este punto, darme salud para lograr mis metas.

A mi Familia.

Dedico el siguiente proyecto a mi familia mis padres que me han apoyado a alcanzar mis metas y a mi esposa que me ha acompañado durante este proceso, a mi hijo que es mi principal motivo para seguir adelante.

William Enrique Salcedo Rodríguez

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia, por permitirme hacer parte de su institución y poder adelantar la especialización en seguridad informática, de igual manera a mis compañeros de curso que me han apoyado, al director de proyectos Fernando Zambrano, al Ingeniero Edgar Roberto Dulce, Ingeniero Jose Hernado Peña. Por su acompañamiento y soporte durante el proceso.

William Enrique Salcedo Rodríguez

CONTENIDO

LISTA DE FIGURAS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

Desarrollar una auditoría interna sobre el sistema de seguridad informático de una entidad estatal como caso de análisis simulado en un ambiente controlado, el cual requiere solución a un problema planteado acerca de dos ciberataques de tipo Defacement y Ransomware.

El objetivo principal de la auditoria es Identificar y analizar las metodologías utilizadas por los black Hackers, que permitieron la materialización de los ciberataques sobre el sistema informático de la entidad estatal, de esta forma diseñar los controles y políticas de seguridad necesarios que minimicen la materialización de nuevos ataques.

Se empleo la metodología de análisis de riesgos MAGERIT para la identificación de activos de hardware y software que presenten vulnerabilidades, sobre las vulnerabilidades encontradas diseñar los controles y políticas necesarias según la norma ISO 27001.

Palabras clave: Black Hackers, Defacement, Ransomware, CGI, Metasploit, Kali Linux, Exploit, Payload, DMZ. Deep web, NMAP, OPENVAS.

ABSTRACT

Develop an internal audit on the computer security system of a state entity as a simulated analysis case in a controlled environment, which requires a solution to a problem posed about two cyberattacks of the Defacement and Ransomware type.

The main objective of the audit is to identify and analyze the methodologies used by black hackers, which allowed cyberattacks to materialize on the state entity's computer system, thus designing the necessary controls and security policies that minimize the materialization of new attacks.

The MAGERIT risk analysis methodology will be used to identify hardware and software assets that present vulnerabilities, based on the vulnerabilities found, design the necessary controls and policies according to ISO 27001 and ISO 27002.

Keywords: Black Hackers, Defacement, Ransomware, CGI, Metasploit, Kali Linux,

Exploit, Payload, DMZ. Deep web, NMAP, OPENVAS.

1 INTRODUCCIÓN

El presente proyecto se realizo como opción de grado de tipo proyecto aplicado en el área de Seguridad informática, el cual estudia el estado actual del SGSI de una entidad estatal como caso de análisis simulado en un ambiente controlado, esta entidad fue blanco de ataques por parte de Black Hackers, quienes materializaron ataques de tipo Defacement y Ransomware en las sedes de esta entidad en dos ciudades principales.

2 DEFINICION DEL PROBLEMA

2.1 PRESENTACION

Los Cyber ataques a empresas reconocidas y entes gubernamentales a nivel mundial se han disparado los últimos años, un estudio pionero en la región, fruto de la colaboración entre el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), la Organización de Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) reveló que del 65% de las empresas entrevistadas, entre el 81% y el 100% de su fuerza laboral cuenta con acceso a Internet (en el sector público el 69%). Aun así, solo el 37% de ellas de los sectores servicios, industria y comercio creen que están preparadas para manejar un incidente digital.

En este estudio, una mirada a los incidentes identificados y notificados permite ver que el sector servicios financieros y banca reporta el 18,3%, educación el 15% y Gobierno - consultoría el 10,2%, y que los temas más detectados son caballos de Troya (14,4%), instalación de software no autorizado (13,8%), Phising (11,2%), Ransomware (7,5%) e ingeniería social (6,1%).[1]

Según este estudio un gran porcentaje de las entidades evaluadas no estarían preparadas ante un ataque de tipo informático, ya sea porque no destinan el presupuesto necesario para fortalecer sus sistemas de gestión de riesgos o por que no creen que este tipo de ataques puedan ser materializados en sus organizaciones. En el presente proyecto se aborda de qué manera se pueden identificar las vulnerabilidades en los sistemas de informacion y como diseñar controles y políticas de seguridad que permitan contrarrestar posibles ataques.

[1] Cano, Jeimy Jose. «Colombia no está preparada ante un ciberataque.» s.f. *Universidad del rosario.* https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/. 04 de 10 de 2020|.

2.2 FORMULACIÓN DEL PROBLEMA

Los sistemas de gestión de seguridad informática en las entidades estatales han presentado fugas de informacion y materialización de ataques de tipo cibernético en los últimos años.

Es necesario revisar las políticas y controles de seguridad existente actualmente en esta entidad, de igual manera se deben de analizar los posibles puntos de entrada que permitieron la materialización de los ataques, los responsables de los procesos de seguridad, con el fin de establecer si una falla humana o acciones voluntarias por parte del personal interno, ayudaron a que se materializaran los ataques sobre los sistemas informáticos de la entidad.

De esta manera se propone a dar respuesta a la siguiente pregunta:

¿De qué manera un análisis de riesgo sobre el sistema de informacion en una entidad estatal permite reducir la materialización de ataques de tipo cibernético?

3 JUSTIFICACIÓN

El presente proyecto busca identificar las vulnerabilidades presentes en el sistema de informacion de la entidad estatal, es importante mejorar el actual sistema de gestión de seguridad de la informacion debido a que es una entidad estatal que almacena millones de registros con informacion confidencial de los ciudadanos de Colombia, la materialización de un ataque sobre el sistema de informacion de la entidad pone en riesgo la confidencialidad, integridad y disponibilidad de la informacion allí alojada, vulnerando la ley de habeas data 1581 del 2012, de igual manera los costos de este ataque son incalculables, afectando la confianza y seguridad de los ciudadanos frente a la seguridad de la entidad estatal, por esta razón es imperativo realizar una auditoría interna sobre el sistema de gestión de seguridad de la información, con el fin de identificar vulnerabilidades, de esta manera proponer un plan de gestión de riesgos con los controles necesarios..

4 ALCANCE Y LIMITACIONES DEL PROYECTO

El siguiente proyecto se desarrollo en un ambiente simulado, estuvo centrado sobre el sistema de seguridad de información de la entidad estatal en sus dos sedes principales.

Se identificaron los riesgos sobre el sistema de informacion de la entidad estatal con el fin de mejorar el SGSI implementado actualmente en la entidad, también se propone la creación de controles y políticas de seguridad basadas en las normas ISO 27001.

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Diseñar las políticas para el control de seguridad informática que permita minimizar riesgos y materialización de nuevas amenazas de ataques, sobre el sistema informático de la entidad estatal en sus dos sedes principales.

5.2 OBJETIVOS ESPECÍFICOS

- Realizar las pruebas de tipo pentesting haciendo uso de las herramientas de auditoria informática, en un ambiente controlado.
- Simular los ataques de tipo Defacement y Ransomware, materializados por los Cyber delincuentes en la entidad estatal.
- Realizar el inventario de activos e Identificación de las vulnerabilidades de seguridad presentes sobre los mismos, haciendo uso de la metodología MAGERIT.
- Generar las políticas de seguridad y los controles necesarios según la norma ISO 27001 que den solución a las vulnerabilidades encontradas.

6 MARCO REFERENCIAL

6.1 ANTECEDENTES

Los Cyber ataques de tipo Defacement y Ransomware hacia entidades privadas y gubernamentales, han crecido exponencialmente en la última década, así como el manejo de la información ha evolucionado gracias a las tecnologías de la información y comunicación, también los métodos delictivos lo han hecho y el auge de los llamados black Hackers ha puesto en Jaque no solo a Pymes sino también a grandes entidades gubernamentales que parecían ser infranqueables.

A continuación, se relacionan algunos referentes identificados con el desarrollo del presente trabajo:

6.1.1 Estrategia para anticipar riesgos y amenazas (AREM)

El resultado de la investigación del ingeniero Jeimy J. Cano, Ph. D, profesor asociado de la Universidad del Rosario, ilustra los frutos de la aplicación de un instrumento que nació en el 2014 producto de su experiencia en la industria financiera y de energía, el cual fue implementado durante tres años en una importante empresa de la industria de energía.

La ventana de AREM (acrónimo de amenazas y riesgos emergentes) resulta de particular interés para las empresas que buscan una posición privilegiada a la hora de enfrentar riesgos conocidos y desconocidos en medio de este panorama de incertidumbre del entorno, de manera que puedan adelantar acciones pertinentes, capitalizar los aprendizajes necesarios y avanzar con la celeridad que demanda el agitado mercado digital actual.

Figura 1 Metodología AREM

Fuente:https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque

Esta perspectiva permite identificar las amenazas o riesgos conocidos, los riesgos focalizados, las amenazas latentes y las amenazas emergentes, ampliando el rango de

acción y efectividad de los controles de seguridad para evitar la materialización de ataques.[2]

6.1.2 Honda detiene su producción mundial tras un ataque de Ransomware

El 7 de junio de 2020, Honda recibió un ataque cibernético que afectó a toda su red y operaciones a nivel global, tanto en el ámbito comercial como en el de fabricación. Desde entonces han detenido la producción y oficinas tratando de encontrar una resolución e identificar a los responsables.

Se cree que el virus es lo que se conoce como el Ransomware “Snake”. Este tipo de ataque involucra a un atacante que encripta los archivos de una compañía para mantenerlos como rehenes, y luego los ofrece a cambio de dinero. Honda se refirió a este como un “ataque importante de Ransomware” en su sistema de alerta interna.[3]

Este tipo de ataques se pueden presentar también en organizaciones grandes con sistemas de seguridad informáticos robustos como la compañía Honda.

6.1.3 Wanna Decryptor: el Ransomware que también ataca en Colombia

Diferentes sistemas de seguridad han reportado más de 45.000 ataques, algunos de ellos en Colombia. En un comunicado expedido por el Ministerio TIC, se confirmó que una entidad pública fue atacada y el mismo ministerio fue infectado.

La empresa más afectada hasta el momento ha sido Telefónica, dueña de Movistar. El Ransomware se filtró en su red de intranet, cifrando toda la información en los computadores y exigiendo dinero a cambio de los datos.[4]

En este caso tenemos un precedente en Colombia de un ataque financiero del tipo Ransomware, de ahí la importancia de realizar el análisis de riesgo a la entidad estatal.

---

[2] Cano, Jeimy Jose. «La ventana de AREM, estrategia para anticipar riesgos y amenazas.» s.f. *universidad del rosario.* https://www.urosario.edu.co/UCD/Colombia-no-esta-preparada-ante-un-ciberataque/. 04 de 10 de 2020.

[3] DPL news. (10 de Junio de 2020). *Honda detiene su producción mundial tras un ataque de ransomware*. Obtenido de DPL News.

[4] Tamayo, Juan. «Empresas y entidades públicas colombianas también son víctimas de ataques de ransomware.» 31 de 05 de 2017. XATAKA Colombia. https://www.xataka.com.co/seguridad/empresas-y-entidades-publicas-colombianas-tambien-son-victimas-de-ataques-de-ransomware.

6.2 MARCO CONTEXTUAL

El marco contextual del presente trabajo se centro en una entidad estatal como caso de análisis simulado en un ambiente controlado.

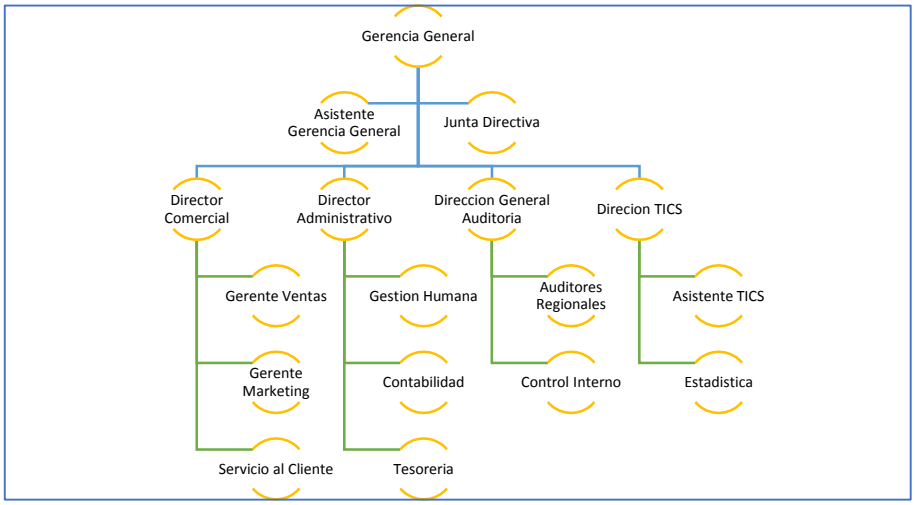
6.2.1 Entidad Estatal

La entidad es de carácter institucional con el objetivo principal de llevar el registro nacional de todos los ciudadanos de Colombia y administrar los procesos electorales a nivel nacional. Es un ente administrativo autónomo con sede principal en la ciudad de Bogotá y sedes descentralizadas en todo el territorio nacional.

6.2.2 Organigrama Entidad Estatal

A continuación se presenta la estructura organizacional de la entidad

Figura 2 Organigrama Entidad estatal



Fuente: William Salcedo Rodríguez

6.2.3 Escenario

Las pruebas de auditoria se hicieron en un ambiente virtual simulando los ataques materializados sobre la entidad estatal.

6.3 MARCO TEÓRICO

En el marco teórico son definidas algunas bases teóricas de la investigación

6.3.1 Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se construye ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información corporativa en las empresas. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Un SGSI es el conjunto de prácticas orientadas a garantizar la seguridad, la integridad y la confidencialidad de los datos.

Los Sistemas de Gestión de la Seguridad de la Información permiten a las organizaciones implementar políticas y procedimientos con el fin de reducir los riesgos de exposición de la información. Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.[5]

6.3.2 Norma ISO 27001

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

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

El eje central de ISO27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales

---

[5] ISO 27001.ES. *SGSI*. s.f. http://www.iso27000.es/sgsi.html#seccion2. 19 de 05 de 2020.

problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.[6]

Sus objetivos son:

- Mantener una imagen excelente tanto interna, como externa (cliente-proveedor).
- Cumplimiento de la legislación vigente.
- Permear con claridad las directrices a seguir para mantener la seguridad de la información y datos,
- Identificación, análisis y mitigación de los riesgos asociados al sistema de información actual de la organización.
- Conocimiento de la importancia que tiene la información para la entidad, con el fin de armonizar la seguridad.
- Mejora procesos, procedimientos y actividades con que se desarrolla la gestión en cuanto a la información.

[6] AMUTIO Gómez, Miguel Angel, Javier CANDAU y Jose Antonio Maña. «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.» 10 de 2012. *Portal de Administración Electrónica.* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=2ahUKEwi7w-urgb_pAhXplOAKHcq7A1EQFjAFegQIBBAB&url=https%3A%2F%2Fwww.ccn-cert.cni.es%2Fdocumentos-publicos%2F1789-magerit-libro-i-metodo%2Ffile.html&usg=AOvVaw1Ptyp6z8gq4timVzvvtxkm.

6.3.3 Dominios del Sistema de Gestión de Seguridad de la Información

Los dominios seleccionados para gestionar la información e implementar el sistema de gestión de seguridad de la información son:

- **Políticas de la seguridad de la información**: Su objetivo es garantizar a la empresa el soporte y gestión necesarios para la seguridad de la información según todos los requisitos institucionales y normativos. Se debe establecer la política según *los* objetivos establecidos por la empresa. Es necesario contar con el compromiso en cuanto a la seguridad de la información.
- **Organización de la seguridad de la información**: El objetivo de este dominio es establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la organización.
- **Seguridad de los recursos humanos**: El objetivo de este dominio es la necesidad de educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.
- **Gestión de activos**: El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.
- **Seguridad física y del entorno**: El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.
- **Seguridad de las operaciones**: El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.
- **Adquisición, desarrollo y mantenimiento de sistemas**: El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.
- **Relaciones con los proveedores**: El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.
- **Gestión de incidentes de seguridad de la información**: El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.
- **Aspectos de seguridad de la información de la gestión de continuidad del negocio**: El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

- **Cumplimiento**: El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.[7]

6.3.4 Método de Análisis de Riesgos Magerit

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- ✓ Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- ✓ Determinar a qué amenazas están expuestos aquellos activos
- ✓ Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- ✓ Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- ✓ Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.
- ✓ Con el objeto de organizar la presentación, se introducen los conceptos de "impacto y riesgo potenciales", Estas valoraciones son "teóricas": en el caso de que no hubiera salvaguarda alguna desplegada. Una vez obtenido este escenario teórico, se incorporan las salvaguardas derivando estimaciones realistas de impacto y riesgo.[8]

- **Activo**: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- **Valoración del activo**: La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes. El valor puede ser propio, o puede ser acumulado. Se dice que los

---

[7] Ibid.;

[8] AMUTIO Gómez, Miguel Angel, Javier CANDAU y Jose Antonio Maña. «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.» 10 de 2012. *Portal de Administración Electrónica.* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=2ahUKEwi7w-urgb_pAhXplOAKHcq7A1EQFjAFegQIBBAB&url=https%3A%2F%2Fwww.ccn-cert.cni.es%2Fdocumentos-publicos%2F1789-magerit-libro-i-metodo%2Ffile.html&usg=AOvVaw1Ptyp6z8gq4timVzvvtxkm.

activos inferiores en un es-quema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

- **Dimensiones**: De un activo puede interesar calibrar diferentes dimensiones:

Confidencialidad: ¿Qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos

Integridad: ¿Qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.

Disponibilidad: ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

- **Amenazas**: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

Identificación de las amenazas: A continuación, se presenta una relación de amenazas típicas.

De origen natural: Hay accidentes naturales (terremotos, inundaciones), ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.

Del entorno (de origen industrial): Hay desastres industriales (contaminación, fallos eléctricos), ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Defectos de las aplicaciones: Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, ‘vulnerabilidades’.

Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

- **Salvaguardas:** Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran implemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras requieren seguridad física y, por último, está la política de personal.

  Ante el amplio abanico de posibles salvaguardas a considerar, es necesario hacer una criba inicial para quedarnos con aquellas que son relevantes para lo que hay que proteger. En esta criba se deben tener en cuenta los siguientes aspectos:

  - Tipo de activos a proteger, pues cada tipo se protege de una forma específica.
  - Dimensión o dimensiones de seguridad que requieren protección
  - Amenazas de las que necesitamos protegernos.
  - Si existen salvaguardas alternativas.

  Además, es prudente establecer un principio de proporcionalidad y tener en cuenta:

  - El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.
  - La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes.
  - La cobertura del riesgo que proporcionan salvaguardas alternativas

- **Tipos de protección:** Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

[PR] Prevención: Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega a ocurrir, los daños son los mismos.

[DR] Disuasión: Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tienen influencia sobre los daños causados caso de que el atacante realmente se atreva.

[EL] Eliminación: Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya

producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

[IM] Minimización del impacto / limitación del impacto: Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

[CR] Corrección: Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo repara. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

[RC] Recuperación: Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

[MN] Monitorización: Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y mejorar el sistema de salvaguardas de cara al futuro.

[DC] Detección: Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

[AW] Concienciación: Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

[AD] Administración: Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que haya puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo. [9]

---

[9] AMUTIO Gómez, Miguel Angel, Javier CANDAU y Jose Antonio Maña. «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.» 10 de 2012. *Portal de Administración Electrónica.* https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&ved=2ahUKEwi7w-urgb_pAhXplOAKHcq7A1EQFjAFegQIBBAB&url=https%3A%2F%2Fwww.ccn-

6.3.5 Malware

Los atacantes pudieron usar métodos de intrusión basados en código malicioso o malware para infiltrarse en los servidores de la registraduría nacional, a continuación, se comparte el termino malware de un blog informático:

"Se puede definir el Malware como la abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo se pueden encontrar términos como: Virus, Troyanos (Trojans), Gusanos (Worm), keyloggers, Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues."[10]

La mejor manera de protección frente a este tipo de software malicioso es tener un sistema de antivirus robusto y actualizado que pueda ser administrado de manera centralizada en un servidor, de esta manera tener control sobre los equipos de la organización. Contar con las últimas actualizaciones de seguridad en los sistemas operativos, protege el equipo corrigiendo errores de seguridad que pueden ser usados por un delincuente informático.

6.3.6 Ataque de Tipo Ransomware

Los ataques de tipo Ransomware materializados sobre la sede de la registradora nacional en la ciudad de Cali, expuso los datos personales de los ciudadanos, a continuación, se comparte el concepto de Ransomware, definición dada por la universidad de JAEN en su revista "Guías de seguridad UJA".

> Se puede definir el Ransomware como un tipo de malware (software malicioso) que bloquea el uso de un dispositivo (ordenador, Tablet, Smartphone...) o la información que contiene, para después pedir un rescate a cambio de su recuperación. El método más habitual de propagación es a través del envío de correos electrónicos maliciosos a las víctimas. Los cibercriminales las engañan para que abran un archivo adjunto infectado o hagan clic en un enlace que los lleva al sitio web del atacante, dónde se infectan. Una vez

---

cert.cni.es%2Fdocumentos-publicos%2F1789-magerit-libro-i-metodo%2Ffile.html&usg=AOvVaw1Ptyp6z8gq4timVzvvtxkm.

[10] RIVERO, Marcelo. *¿ Que son los Malwares ?* [En linea]. 01 de 10 de 2016. (Consultado:26 de abril de 2020). https://www.infospyware.com/articulos/que-son-los-malwares.

infectados, mediante un mensaje, que suele ser intimidante, avisan a la víctima de que la única forma en que puede descifrar sus archivos o recuperar el sistema es pagar al cibercriminal.[11]

Este tipo de ataques son muy comunes actualmente afectando a miles de personas y empresas, las organizaciones han tomado sus medidas de control para evitar este tipo de ataques, entre las principales políticas de seguridad están:

- Copias de seguridad de la información critica
- Actualizaciones de seguridad en el sistema operativo
- Evitar sitios web de contenido dudoso
- Concientizar a los usuarios frente a este tipo de ataques.

6.3.7 Ataque de Tipo Defacement

Los ataques tipo Defacement tienen como objetivo sitios o plataformas web, buscando des configurar su aspecto o alterando el acceso a estas, poniendo en riesgo la disponibilidad de la información que es alojada en estos sitios web. A continuación, se enuncian algunas políticas que se pueden aplicar al ser víctimas de este tipo de ataques.

- Instaurar en la organización una política de actualizaciones, así el gestor de contenidos web estará protegido frente a las vulnerabilidades conocidas.
- También es necesaria una política de contraseñas.
- Utilizar herramientas de análisis de seguridad y de vulnerabilidades.
- Establecer periodos de revisión de seguridad del portal web.
- Realizar copias de seguridad de la página periódicamente y salvaguardarlas en un lugar diferente al origen de los datos.
- Verificar regularmente que las copias se realizan correctamente y que pueden restaurarse.
- Crear conciencia a los empleados en materia de seguridad, un empleado formado podría reconocer las trampas de los Cyber delincuentes.[12]

---

[11] UNIVERSIDAD DE JAEN. «Guias de seguridad UJA - Ransomware.» 01 de 02 de 2018. (Consultado:26 de 04 de 2020). Disponible en: <https://www.ujaen.es/servicios/sinformática/sites/servicio_sinformática/files/uploads/guiaspracticas/Triptico%20de%20seguridad%20UJA%20-%206.%20Ransomware.pdf>.

[12] INCIBE. «INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD.» 25 de 04 de 2019. (Consultado: 26 de 04 de 2020.) Disponible en: https://www.incibe.es/protege-tu-empresa/blog/protegete-frente-al-defacement-y-no-le-cambien-cara-tu-web.

6.4 MARCO CONCEPTUAL

En el marco conceptual se encuentran los términos principales que facilitaron la compresión de la investigación llevada a cabo.

6.4.1 Servidor Web Apache

Los servidores web de la entidad estatal están desarrollados sobre plataforma web Apache, a continuación, son definidas las características del servidor web apache.

"Aunque Apache sea conocido como un servidor web, no es un servidor físico, sino un software que se ejecuta en un servidor. Su trabajo es establecer una conexión entre un servidor y los navegadores de los visitantes del sitio web (Firefox, Google Chrome, Safari, etc.) mientras envían archivos entre ellos (estructura cliente-servidor). Apache es un software multiplataforma, por lo cual funciona tanto en servidores Unix como en Windows."[13]

6.4.2 DMZ (Zona Desmilitarizada)

"Una red DMZ corresponde a una red segura y aislada del resto. Es una red que está aislada del resto de redes de la empresa (incluyendo la red interna) y en la que se controla cualquier tráfico que se establezca con el resto. Es un terreno neutral que separa los recursos de varias redes. El acceso a esta red es restringido y limitado exclusivamente a los servicios a los que los usuarios pueden acceder." [14]

En una red DMZ solo deben de estar ubicados servidores web y plataformas a los cuales se pueda tener acceso desde una red WAN, pero no deben de estar ubicados en este DMZ servidores o plataformas con un mayor grado de confidencialidad, por ejemplo, servidores de Bases de datos o aplicaciones.

Es recomendable que se configure un segmento de red diferente para los servidores ubicados en la DMZ y los hosts que hacen parte de la red local, esta es una buena práctica que minimiza el riesgo de acceso no autorizado a nuestra red interna.

---

[13] B, Gustavo. «¿Qué es Apache? .» 01 de 11 de 2019. *Hostinger tutoriales.*(Consultado: 26 de 04 de 2020).Disponible en: https://www.hostinger.co/tutoriales/que-es-apache/.

[14] DIGITAL GUIDES IONOS. «DIGITAL GUIDES IONOS.» 17 de 10 de 2016. *¿En qué consiste una zona desmilitarizada (DMZ)?* https://www.ionos.es/digitalguide/servidores/seguridad/en-que-consiste-una-

6.4.3 Metasploit

Una de las técnicas que puede utilizar el atacante para acceder a los servidores web de la Registradora nacional, son el uso de software de ataque de vulnerabilidades de tipo Metasploit, el cual es definido a continuación.

“Metasploit es un proyecto de código abierto para la seguridad informática, que proporciona información acerca de vulnerabilidades de seguridad y ayuda en test de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.” [15]

Es posible acceder a esta herramienta de escaneo y ataque de vulnerabilidades por medio del Framework de Metasploit incluido en el software de auditoria informática Kali Linux.

6.4.4 Exploit

En el medio Hacking es muy conocido el uso de Exploits, los Cyber delincuentes que materializaron los ataques sobre los servidores de la registradora nacional probablemente hicieron uso de algunos Exploits, a continuación, es definido el concepto de Exploit.

“Un Exploit es un ataque poco ético o ilegal que se aprovecha de las vulnerabilidades de las aplicaciones, las redes o el hardware. Este ataque se suele materializar en software o código que tienen como objetivo obtener el control de un sistema informático o robar datos guardados en una red ”.[16]

Básicamente un Exploit es un fragmento de código malicioso diseñado para atacar una vulnerabilidad específica, el framework de Metasploit permite ejecutar los Exploit y así poder atacar las vulnerabilidades.

6.4.5 Zennmap

---

[15] Wikipedia. *"Metasploit." Wikipedia.* 17 de 04 de 2020.(Consultado: 26 de 04 de 2020). Disponible en: https://es.wikipedia.org/w/index.php?title=Metasploit&oldid=125273584.

[16] s.r.o., AVAST Software. *¿Qué son los exploits?* s.f. https://www.avast.com/es-es/c-exploits. 26 de 04 de 2020. <https://www.avast.com/es-es/c-exploits>.

Entre las herramientas de auditoria informática utilizada por los Cyber delincuentes, el NMAP es una de las herramientas básicas en el escaneo de puertos, la cual con su interfaz gráfica ZENMAP facilita su uso.

“ZENMAP es la interfaz gráfica oficial de NMAP, el conocido programa de código abierto para hacer escaneo de puertos a fondo de cualquier equipo conectado. ZENMAP proporciona una interfaz gráfica para ejecutar los diferentes tipos de análisis de puertos que tiene NMAP y también para mostrarlos de forma intuitiva a los usuarios menos experimentados”.[17]

Esta herramienta de auditoria informática es de gran ayuda no solo en la identificación de puertos, sino que también identifica características como sistemas operativos, nombre de host, direcciones MAC, entre otras características que pueden ser de provecho para un atacante.

6.4.6 Openvas

El framework OPENVAS permite escanear múltiples vulnerabilidades en diferentes plataformas, tal cual como lo indica su sitio web oficial.

“OPENVAS es un framework de varios servicios y herramientas que ofrece una solución completa y potente de exploración de vulnerabilidades y gestión de vulnerabilidades. El framework forma parte de la solución de gestión de vulnerabilidad comercial de Greenbone Networks, desde la cual se contribuyen los desarrollos a la comunidad Open Source desde 2009.”[18]

La suite de OPENVAS tiene múltiples ventajas, no solo identifica vulnerabilidades, también indica que Exploits se recomiendan para atacar estas vulnerabilidades y las recomendaciones de seguridad para corregir estas vulnerabilidades, ósea que puede ser usado de manera ética para corregir vulnerabilidades o de manera ilegal como lo podría hacer un Cyber delincuente.

---

[17] DE LUZ, Sergio. *Redes Zone - ZENMAP*. 18 de 01 de 2014. https://www.redeszone.net/2014/01/18/ZENMAP-la-interfaz-grafica-oficial-de-NMAP-para-escanear-puertos-a-fondo/. 26 de 04 de 2020.

[18] Open Vas. *OPENVAS - Open Vulnerability Assessment Scanner*. s.f. https://www.OPENVAS.org/. 26 de 04 de 2020.

6.5 MARCO LEGAL

En esta fase se indican las leyes, normas y decretos, que son el fundamento legal para la investigación que se llevo a cabo.

6.5.1 Ley 1266 de 2008

Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

6.5.2 LEY 1273 DE 2009

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

6.5.3 Ley 1437 de 2011

Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

6.5.4 Ley 1581 de 2012

Por la cual se dictan disposiciones generales para la protección de datos personales.

6.5.5 Decreto 3816 de 2003

Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública.

6.5.6 Decreto 235 de 2010

Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones.

6.5.7 Decreto 019 de 2012

Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

6.5.8 Decreto 2609 de 2012

Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

6.5.9 Decreto 1078 de 2015

Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnología de la Información y las Comunicaciones" [19]

6.5.10 Decreto 2559 de 2015

Por el cual se fusiona la Agencia Nacional para la Superación de la Pobreza Extrema ANSPE y la Unidad Administrativa Especial para la Consolidación Territorial - UACT en el Departamento Administrativo para la Social Prosperidad Social y se modifica su estructura.

6.5.11 Decreto 415 de 2016

"Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones"

6.5.12 Decreto 2094 de 2016

Por el cual se modifica la estructura del Departamento Administrativo para la Prosperidad Social - Prosperidad Social.

6.5.13 Decreto 1499 de 2017

Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.[20]

---

[19] SENADO, SECRETARIA. «secretariasenado.gov.co.» 31 de 12 de 2019. http://www.secretariasenado.gov.co/senado/basedoc/arbol/1000.html. 26 de 04 de 2020.

[20] Ibid.;

7 DISEÑO METODOLÓGICO

Se hizo uso de la metodología MAGERIT en el análisis de riesgo sobre el sistema de informacion, esta metodología es muy útil debido a que nos permitio realizar de manera ordenada las siguientes fases:

7.1 FASE 1 IDENTIFICACIÓN DE ACTIVOS

En esta fase se identificaron los activos principales de la entidad estatal en sus sedes principal y secundaria. La nomenclatura de los activos se basa en la metodología MAGERIT, clasificando los activos de la siguiente manera:

- [D] - Datos/Informacion
- [S] - Inventario de servicios
- [SW] - Aplicaciones informáticas – Software
- [HW] - Equipos informáticos
- [COM] - Redes de comunicaciones
- [MEDIA] - Soportes de Información. Electrónico/No Electrónico
- [AUX] - Equipamiento Auxiliar:
- [L] - Instalaciones
- [P] – Personal.

7.2 FASE 2 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

En la siguiente fase se identifican las principales amenazas sobre los activos, según la clasificación del método de análisis y gestión de riesgo MAGERIT. Entre las principales amenazas que se pueden presentar, está la siguiente clasificación:

- [N] - Desastres naturales
- [I] - De Origen Industrial
- [E] - Errores y fallos no intencionados
- [A] - Ataques intencionados

7.3 FASE 3 DISEÑO DE CONTROLES DE SEGURIDAD

Una vez realizado el inventario de activos, e identificadas las amenazas y vulnerabilidades, el siguiente paso es diseñar los controles que permitirán reducir el riesgo. Las salvaguardas están definidas por la norma ISO 27001, según la amenaza identificada, el tipo de tratamiento a implementar está definido por el método de gestión de riesgos MAGERIT.

8 ALISTAMIENTO ENTORNO DE PRUEBAS

Después de haberse identificado el problema, plantear el alcance, objetivos metodología a emplear, se realizo el desarrollo de la auditoria sobre el sistema informático de la entidad estatal en un escenario controlado.

Primero es simulado el ataque realizado por los Black Hackers sobre la entidad estatal, haciendo uso de herramientas de software forenses como el Kali Linux.

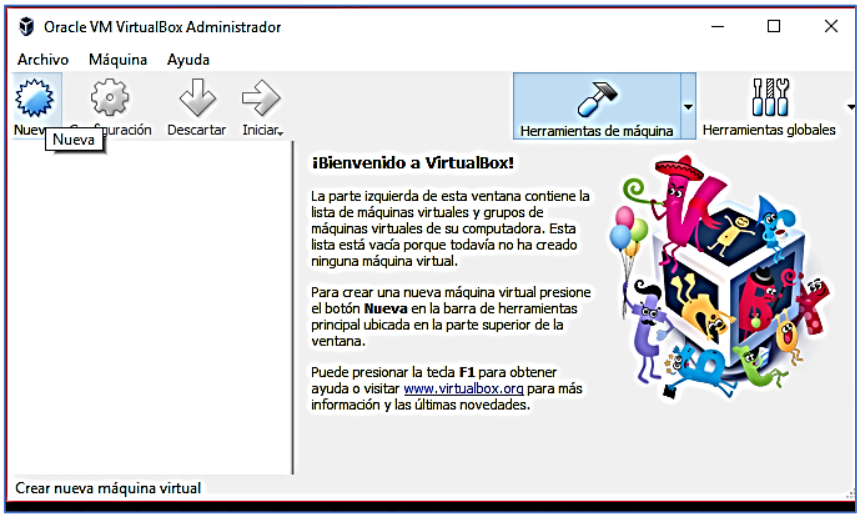
8.1 Instalación de las Máquinas Virtuales

Se descarga la herramienta de virtualización VirtualBox, la cual se puede obtener en el siguiente enlace: https://www.VirtualBox.org/ se descarga la versión de 32 o 64 bits, en este caso la versión de 64 bits. Una vez se tenga la aplicación descargada, se procede a instalar de manera tradicional en el directorio local de preferencia, por defecto se instala en el disco raíz del sistema.

8.1.1 Instalación del Servidor Kali Linux

El siguiente paso es configurar la máquina virtual sobre la cual se instalo el sistema Kali Linux. Se ejecuta el Virtual Box creando una nueva máquina virtual y seleccionando el tipo de plataforma Linux, la figura 3 muestra la interfaz principal del Virtual Box.

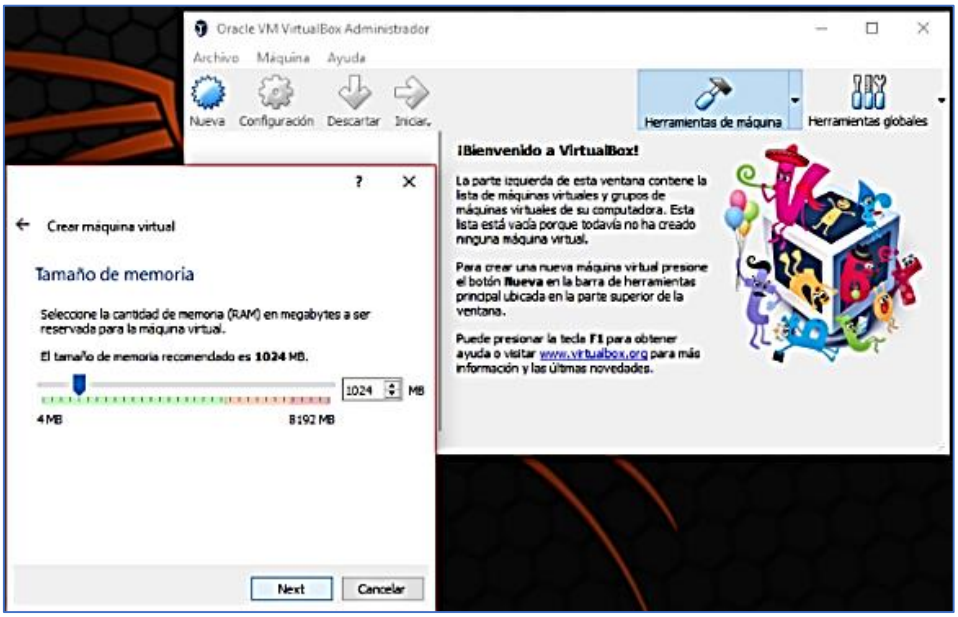
Figura 3 Interfaz principal VirtualBox



Fuente: William Salcedo Rodríguez

Se asigna el espacio en memoria requerido, en la figura 4 se puede apreciar que se asignaron 1024 Mb de memoria.

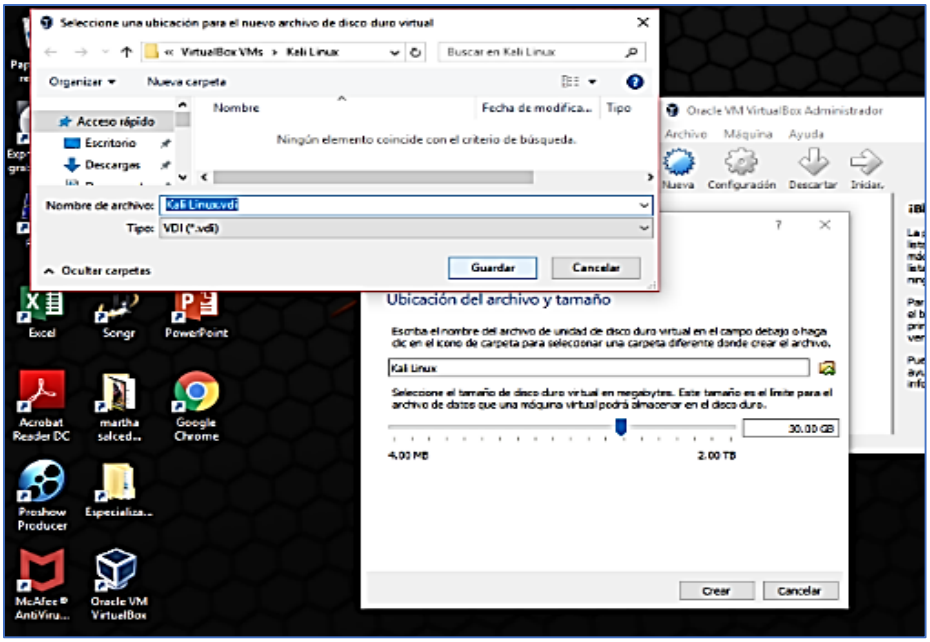
Figura 4 Configuración espacio en memoria Kali Linux



Fuente: William Salcedo Rodríguez

Después se crea la unidad de disco virtual, seleccionando el tipo de disco virtual, el tamaño y la ubicación para guardar, en la figura 5 es seleccionado el disco de 30 Gb de tamaño.

Figura 5 Configuración del disco duro Kali Linux



Fuente: William Salcedo Rodríguez

De esta manera se creo la máquina virtual para poder proceder con la instalación del servidor Kali Linux, la figura 6 muestra la maquina Kali Linux creada.

Figura 6 Máquina Virtual Kali Linux creada

Fuente: William Salcedo Rodríguez

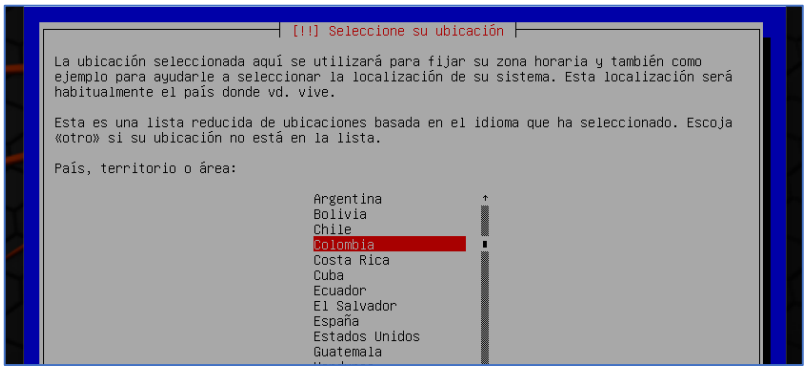
Se ejecuta la máquina virtual creada y se ubica la imagen del sistema Kali Linux, el cual ha sido descargado previamente, se da la opción de instalar, la figura 7 muestra la interfaz de instalación de Kali Linux.

Figura 7 Instalar sistema Kali Linux desde imagen ISO

Fuente: William Salcedo Rodríguez

Después se selecciona ubicación e idioma de instalación en Kali Linux, en la figura 8 escogemos el territorio Colombia.

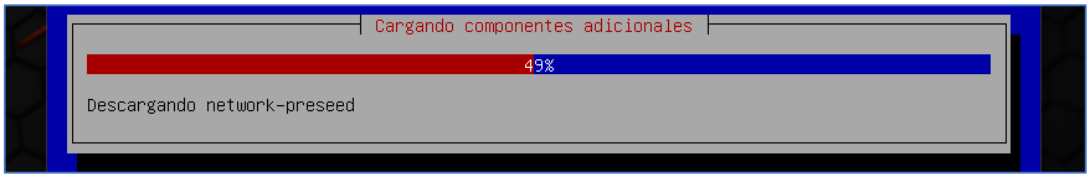
Figura 8 Ubicación e idioma



Fuente: William Salcedo Rodríguez

El sistema descarga los paquetes necesarios para terminar la instalación del sistema operativo Kali Linux, en la figura 9 se evidencia la descarga de paquetes.

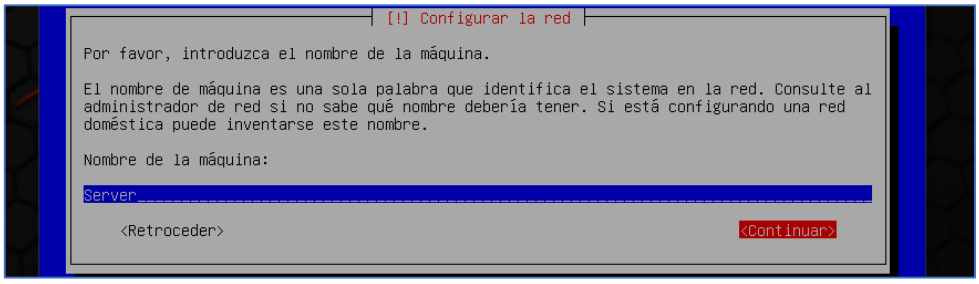
Figura 9 Descarga de paquetes



Fuente: William Salcedo Rodríguez

El siguiente paso es la configuración de red, escribimos el nombre del servidor, en la figura 10 se evidencia el nombre asignado, en este caso es SERVER.

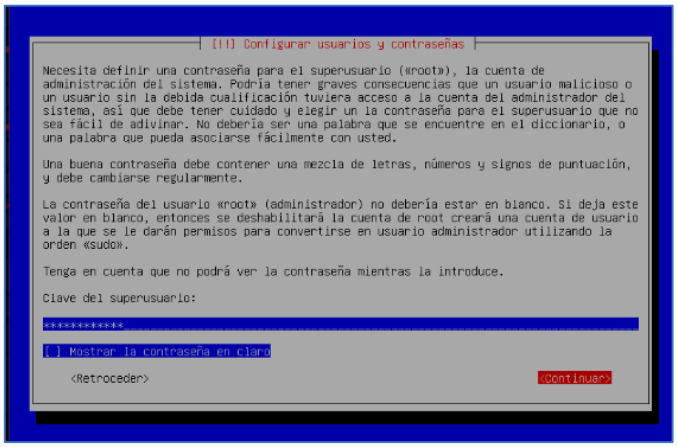
Figura 10 Configuración red Kali Linux



Fuente: William Salcedo Rodríguez

El siguiente paso se configura el usuario, para lo cual se ingresa el usuario y la contraseña, este usuario es diferente al usuario root el cual ya viene configurado por defecto. En la figura 11 se evidencia la creación del usuario.

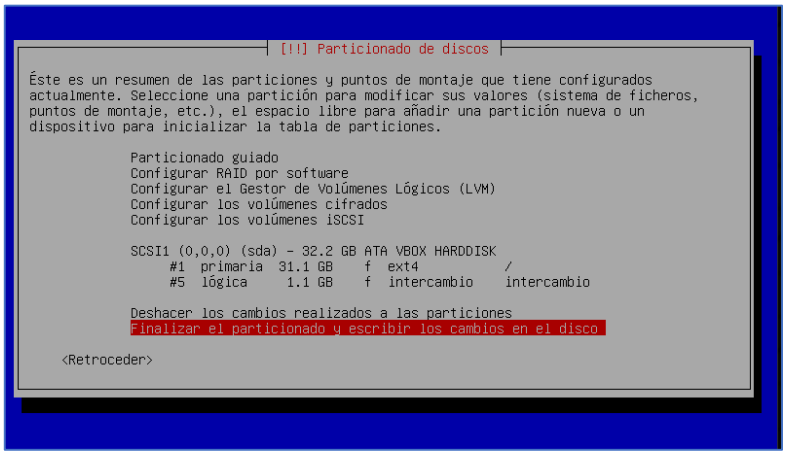
Figura 11 Configuración Usuario Kali Linux



Fuente: William Salcedo Rodríguez

El siguiente paso es configurar las particiones de arranque del sistema Kali Linux, en la figura 12 se evidencia la unidad primaria de 30 Gb con sistema de archivos ext4.

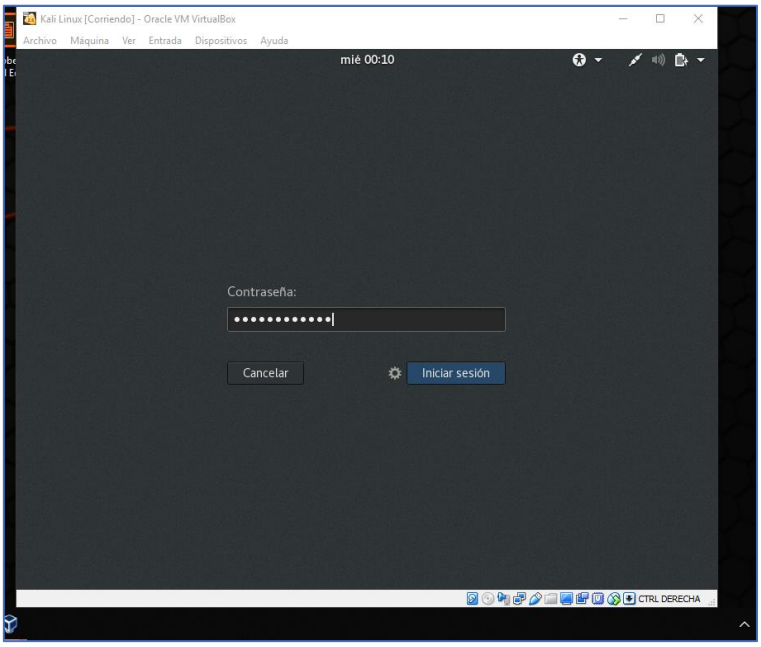
Figura 12 Configuración particiones de arranque Kali Linux



Fuente: William Salcedo Rodríguez

La instalación tarda unos minutos más, se reinicia y solicita las credenciales de ingreso que se han configurado previamente. Ya se puede ingresar con el usuario root o con el usuario configurado, la figura 13 muestra la interfaz de inicio de Kali Linux para ingresar con el usuario.

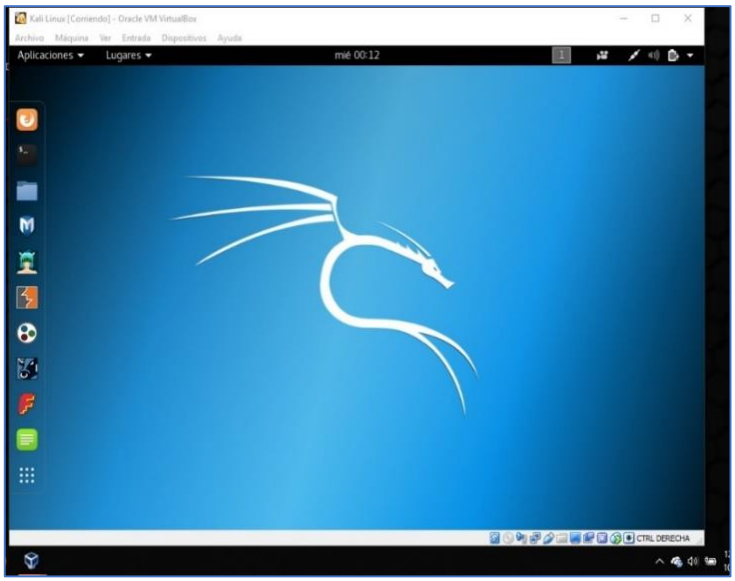
Figura 13 Interfaz Inicio Kali Linux



Fuente: William Salcedo Rodríguez

Finalmente, el sistema ingresa y muestra el escritorio principal, la figura 14 muestra el escritorio principal del Kali Linux.

Figura 14 Escritorio principal Kali Linux

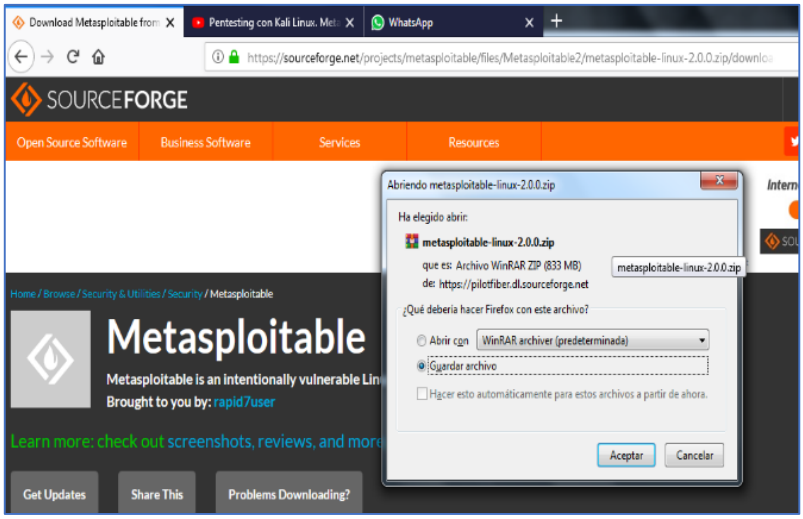


Fuente: William Salcedo Rodríguez

8.1.2 Instalación del Servidor Metasploitable

A continuación, se instala el sistema operativo Metasploitable, se descarga la imagen ISO de la distribución de Linux Metasploitable, la figura 15 muestra la página en la cual se descarga la ISO Metasploitable.

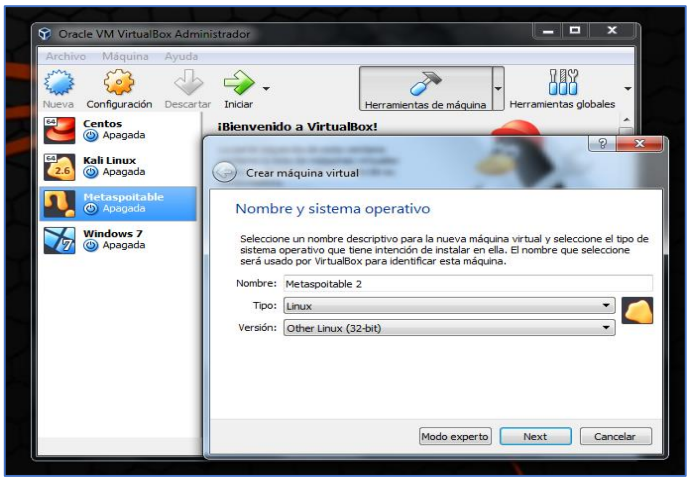
Figura 15 Descarga ISO sistema Metasploitable



Fuente: William Salcedo Rodríguez

El siguiente paso es configurar la máquina virtual sobre la cual se instala el servidor Metasploitable. En la figura 16 se crea la nueva máquina virtual, seleccionando el tipo de plataforma Linux.

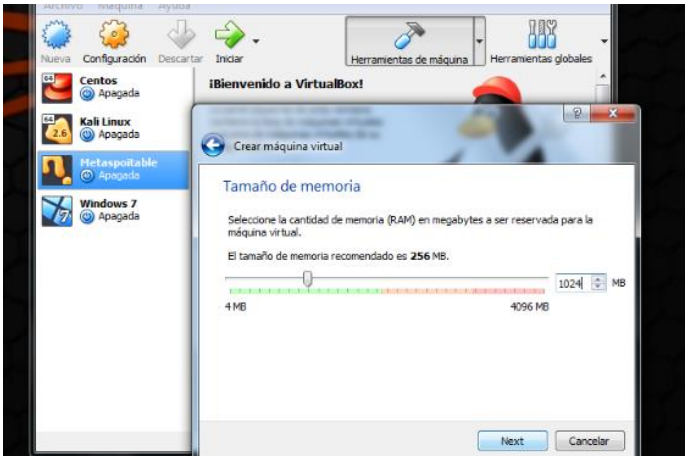
Figura 16 Nueva máquina virtual tipo Linux



Fuente: William Salcedo Rodríguez

Se asigna el espacio de memoria y disco duro requerido para la instalación del sistema Metasploitable, la figura 17 muestra el tamaño de la memoria asignada de 1024 Mb.

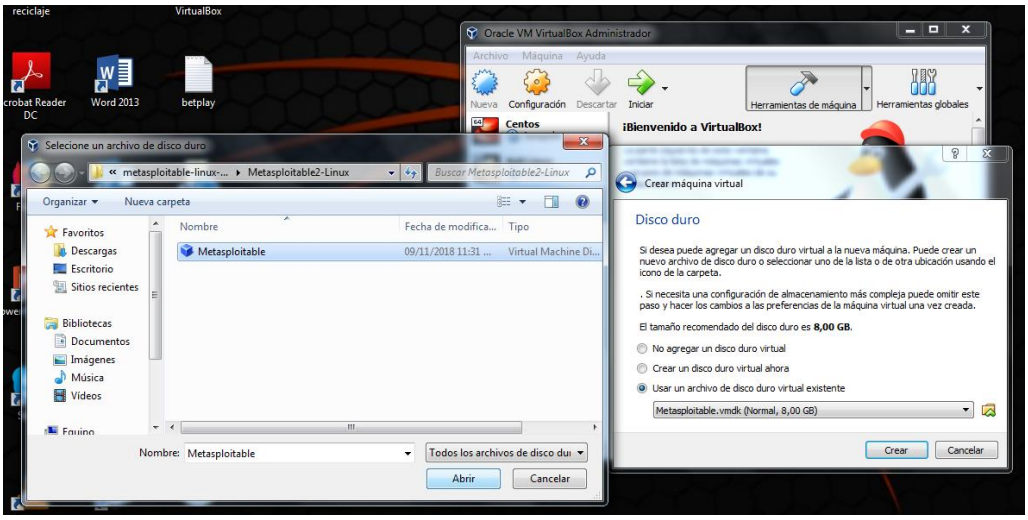
Figura 17 Configuración memoria máquina Metasploitable



Fuente: William Salcedo Rodríguez

En la figura 18 es seleccionada la imagen de la distribución Metasploitable que se ha descargado previamente y se da crear.

Figura 18 Configuración ISO máquina Metasploitable



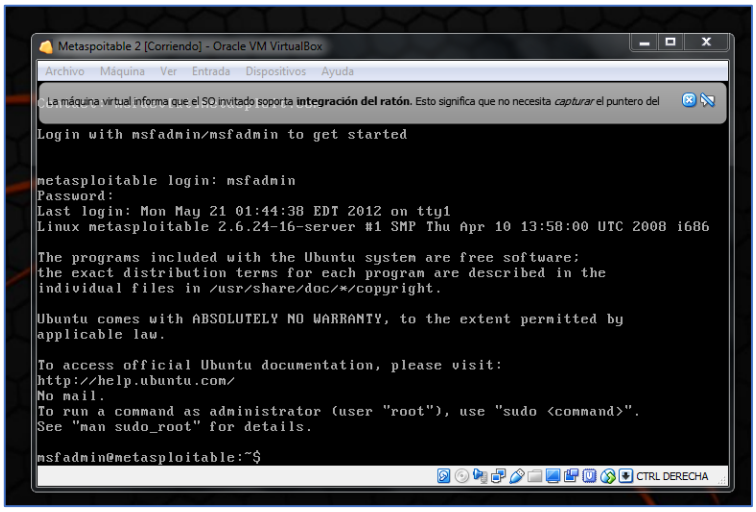
Fuente: William Salcedo Rodríguez

Una vez creada se ejecuta y después de que se inicien todos los respectivos servicios se solicitan datos de acceso, en la figura 19 se evidencia el ingreso al servidor Metasploitable con las siguientes credenciales.

Login: msfadmin

Password: msfadmin

Figura 19 Interfaz inicio servidor Metasploitable



Fuente: William Salcedo Rodríguez

De esta manera se han configurado los servidores Metasploitable y Kali Linux en un entorno virtual por medio de la herramienta de virtualización VirtualBox, sobre estas máquinas podemos realizar las pruebas de pentesting en un ambiente controlado.

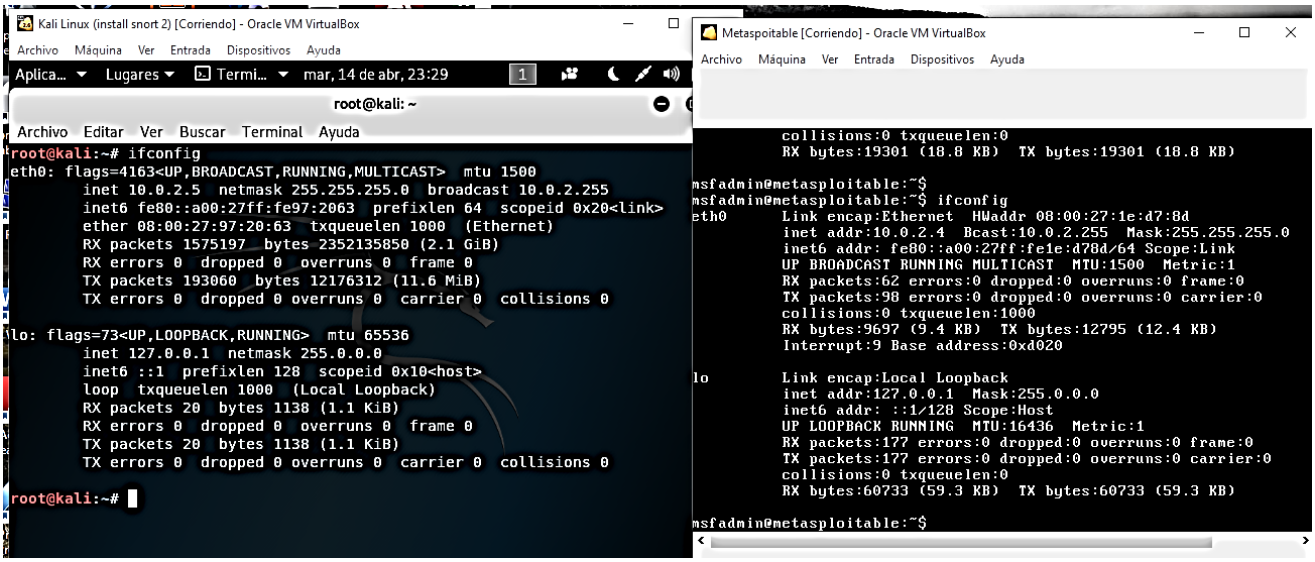
9 PRUEBAS DE PENTESTING EN AMBIENTE CONTROLADO

Las pruebas de pentesting que se realizon son de tipo Black Box, ya que se tiene informacion básica de la entidad como es su topología de red y arquitectura de seguridad existente, pero siguiendo las características de un ataque externo, buscando vulnerabilidades en el sistema de informacion y poder atacar y materializar una amenaza de tipo Ransomware o Defacement.

Una vez se tienen las máquinas virtuales configuradas con el sistema de auditoria Informática Kali Linux y el servidor Metasploitable, el cual hizo las veces del servidor web de la entidad estatal simulada, se procede a realizar las pruebas de pentesting.

Antes de realizar las pruebas de pentesting se verifica que el servidor Metasploitable sobre el cual se hacen los ataques y el servidor Kali Linux desde el cual se hacen los ataques, estén en el mismo segmento de red, ingresando la siguiente instrucción en la línea de comandos *#ifconfig*, en la figura 20 se evidencian las direcciones IP asignadas a cada máquina virtual.

Figura 20 Comando # ifconfig configuración IP



Fuente: William Salcedo Rodríguez

El comando da como resultado la configuración IP del servidor Kali Linux y la máquina Metasploitable:

Kali Linux: 10.0.2.5

Metasploitable: 10.0.2.4

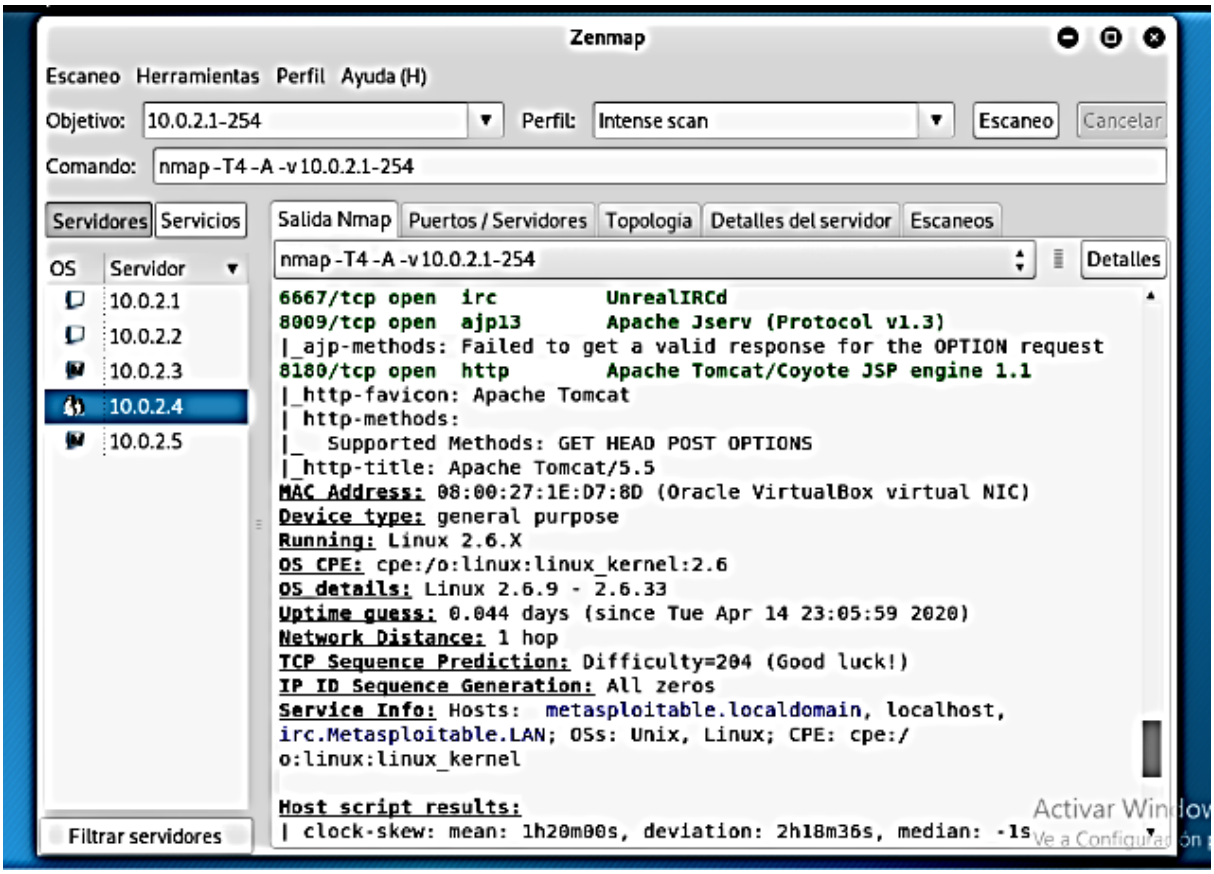
De esta forma se tienen las máquinas configuradas para simular los ataques realizados por los Black Hackers sobre los servidores web de la entidad estatal en sus sedes principal y secundaria.

9.1 Escaneo con Zenmap

Se puede obtener a través de herramientas de auditoria informática como el ZENMAP, las direcciones IP en una determinada red, esto puede hacerse desde la red interna de la entidad o de manera externa si logra infectar e infiltrarse a través de un malware en la red de la organización.

La figura 21 muestra el escaneo realizado con el ZENMAP sobre el segmento 10.0.2.1 – 254.

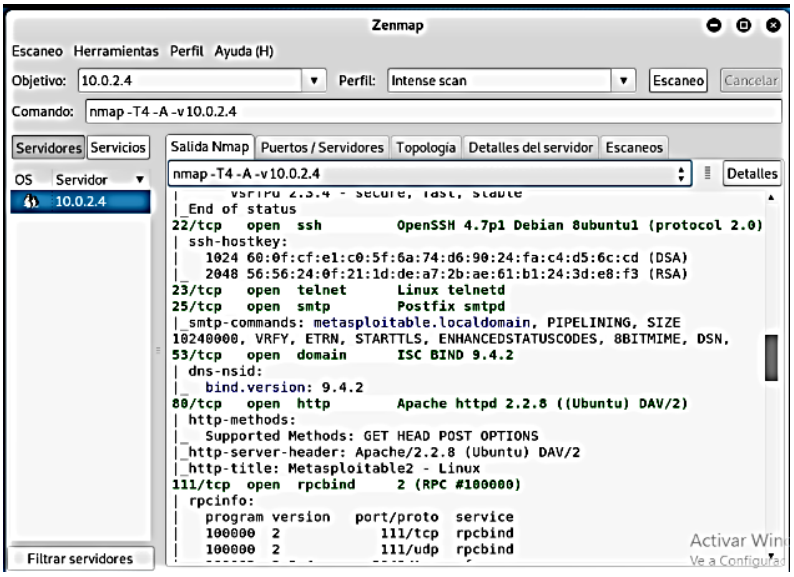
Figura 21 Escaneo ZENMAP



Fuente: William Salcedo Rodríguez

El resultado del ZENMAP muestra un listado con posibles objetivos, entre estos un HOST con plataforma Linux y dirección IP 10.0.2.4, en la figura 22 se realiza un segundo escaneo sobre la dirección IP 10.0.2.4.

Figura 22 Escaneo ZENMAP 10.0.2.4



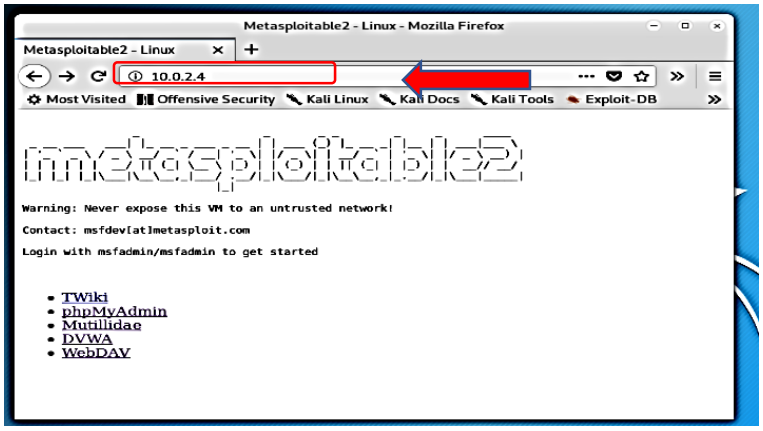
Fuente: William Salcedo Rodríguez

El resultado del escaneo sobre el HOST 10.0.2.4 permite identificar el tipo de plataforma, los servicios que están activos, puertos y otros detalles que le sirven al atacante para perpetrar los ataques.

9.2 Prueba de Acceso por Navegador Web

La siguiente prueba de auditoria consiste en verificar a través del navegador si el HOST 10.0.2.4 apunta hacia algún servidor o plataforma web. En la figura 23 se evidencio que al ingresar la dirección IP 10.0.2.4 en el navegador web se obtiene la siguiente página principal o Índex.

Figura 23 Página Principal Metasploitable



Fuente: William Salcedo Rodríguez

De esta forma se ha encontrado un objetivo, un servidor web el cual aloja una aplicación web. En la figura 24 se accede a la interfaz de la aplicación web DVWA.

Figura 24 Interfaz aplicación Web

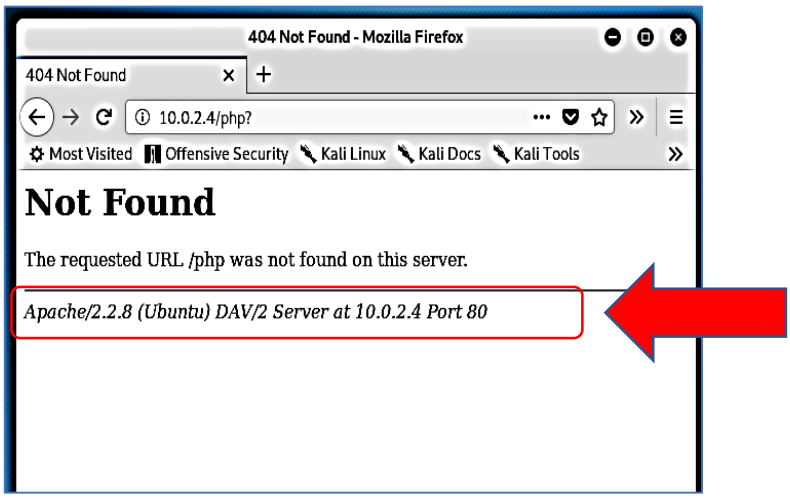
Fuente: William Salcedo Rodríguez

9.3 Identificacion de Tipo de Servidor Web

En la siguiente prueba, a través del navegador web se identifico sobre qué tipo de plataforma están desarrollados los sitios web de la entidad estatal.

En la figura 25 se ingresa el texto .php? en el navegador web, después de la dirección del servidor que es atacado, de la siguiente manera.

Figura 25 Identificación de servidor Apache



Fuente: William Salcedo Rodríguez

De esta forma se confirma que el servidor web está instalado sobre una plataforma Linux, variación de un Ubuntu, también se identifica que existe un servidor HTTP Apache versión 2.2.8 a través del puerto 80.

9.4 Prueba de Acceso a PhpMyAdmin

Una vez que se ha identificado que el sitio web que posiblemente este configurado con lenguaje PHP, ejecutamos la ruta para ingresar desde el navegador web: 10.0.2.4/phpMyAdmin/, en la figura 26 se evidencia la interfaz de acceso al phpMyAdmin.

Figura 26 Interfaz phpMyAdmin

Fuente: William Salcedo Rodríguez

9.5 Escaneo de Vulnerabilidades con Openvas

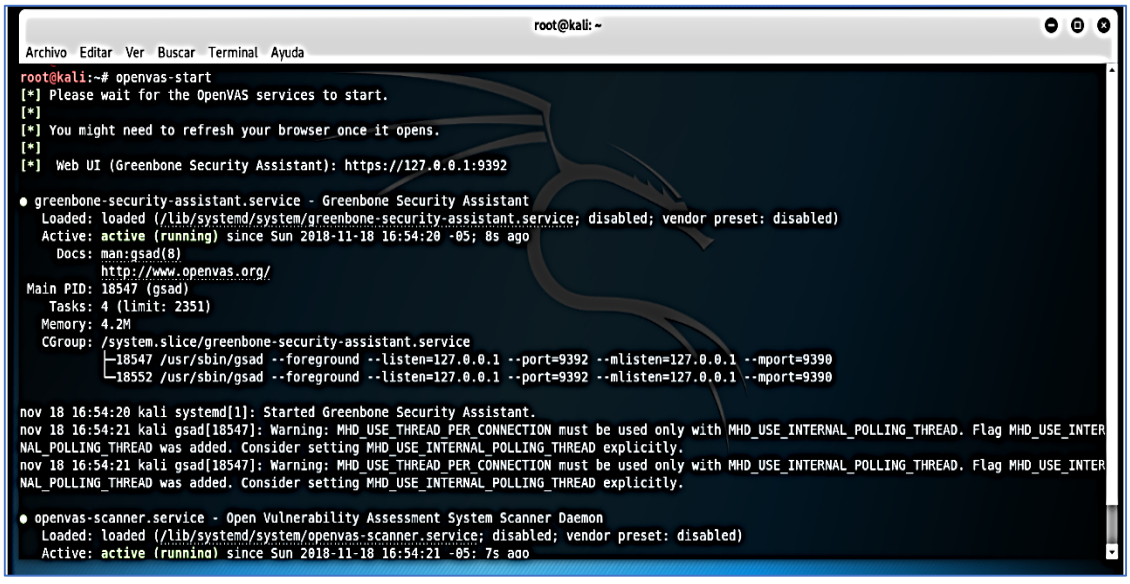
En la siguiente prueba se hizo uso de la herramienta de identificación de vulnerabilidades OPENVAS, la cual viene incluida en la suite del sistema Kali Linux, el primer paso es la instalación del servicio OPENVAS, lo cual se puede realizar desde la terminal del Kali Linux, ejecutando el siguiente comando: *Apt-get install OPENVAS*, la figura 27 muestra la instalación de la herramienta OPENVAS.

Figura 27 Instalación servicio OPENVAS

Fuente: William Salcedo Rodríguez

Una vez ha sido instalado el servicio OPENVAS, se inicia con el siguiente comando: *OPENVAS-start*, la figura 28 muestra el inicio del servicio OPENVAS.

Figura 28 Iniciar servicio OPENVAS



Fuente: William Salcedo Rodríguez

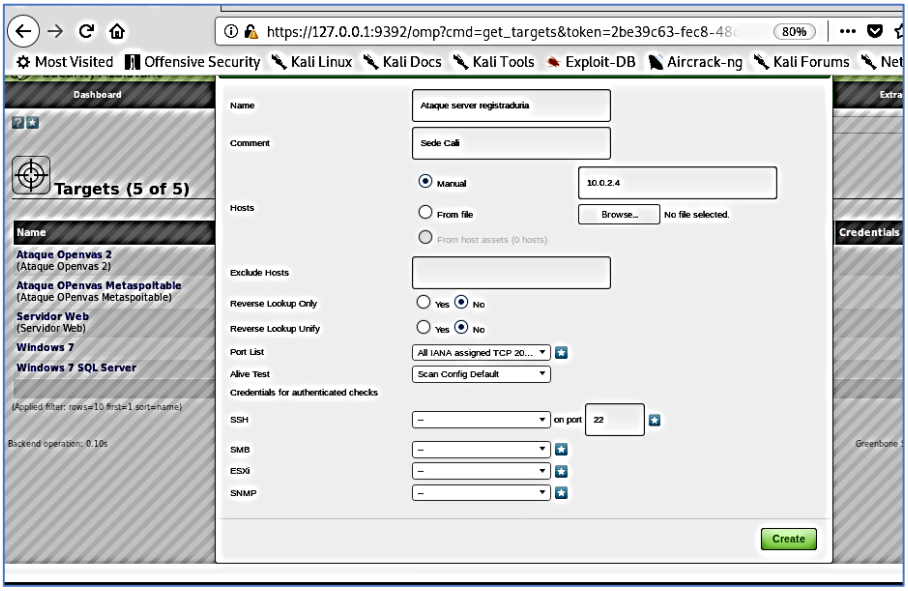
La figura 29 muestra la interfaz de inicio de OPENVAS, la cual es accesible al ingresar la siguiente dirección en el navegador web: https://127.0.0.1:9392

Figura 29 Interfaz inicio Plataforma OPENVAS

Fuente: William Salcedo Rodríguez

Se ingresa al administrador del OPENVAS y se configura el escáner contra la máquina Metasploitable de la siguiente manera. En configuración se crea el nuevo target (Objetivo) digitando la dirección IP de la máquina a escanear (Metasploitable), se da un nombre al objetivo y después de guarda, la figura 30 muestra la creación del objetivo en OPENVAS.

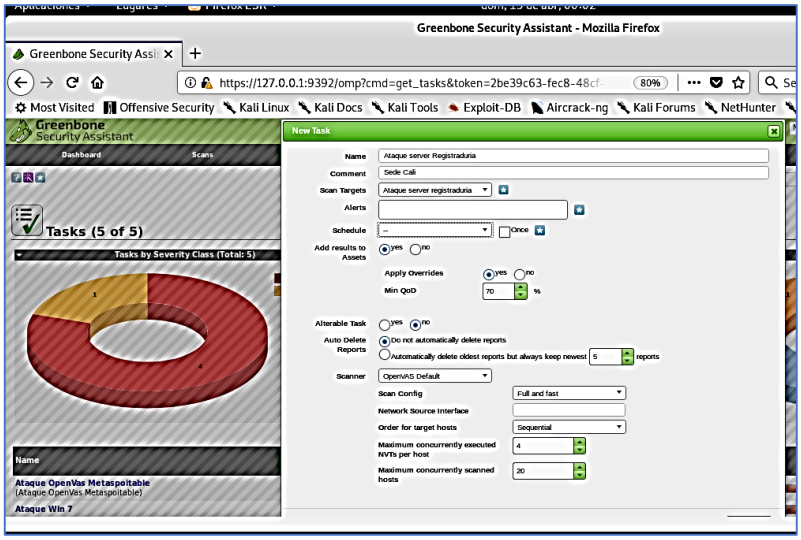
Figura 30 Configuración objetivo plataforma OPENVAS



Fuente: William Salcedo Rodríguez

Una vez ha sido creado el TARGET, se configura el escaneo, ingresando a la pestaña TASK, se da nuevo TASK, seleccionando el target creado anteriormente y guardando el escaneo con un nombre, la figura 31 muestra la creación del objetivo en OPENVAS.

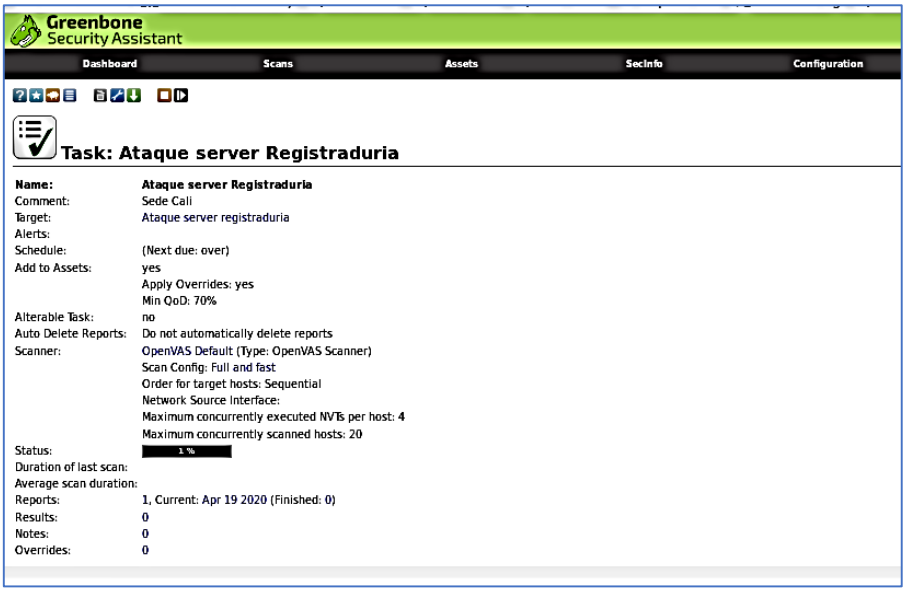
Figura 31 Configuración escaneo en plataforma OPENVAS



Fuente: William Salcedo Rodríguez

En la figura 32 se puede ver el escáner sobre el objetivo ya configurado

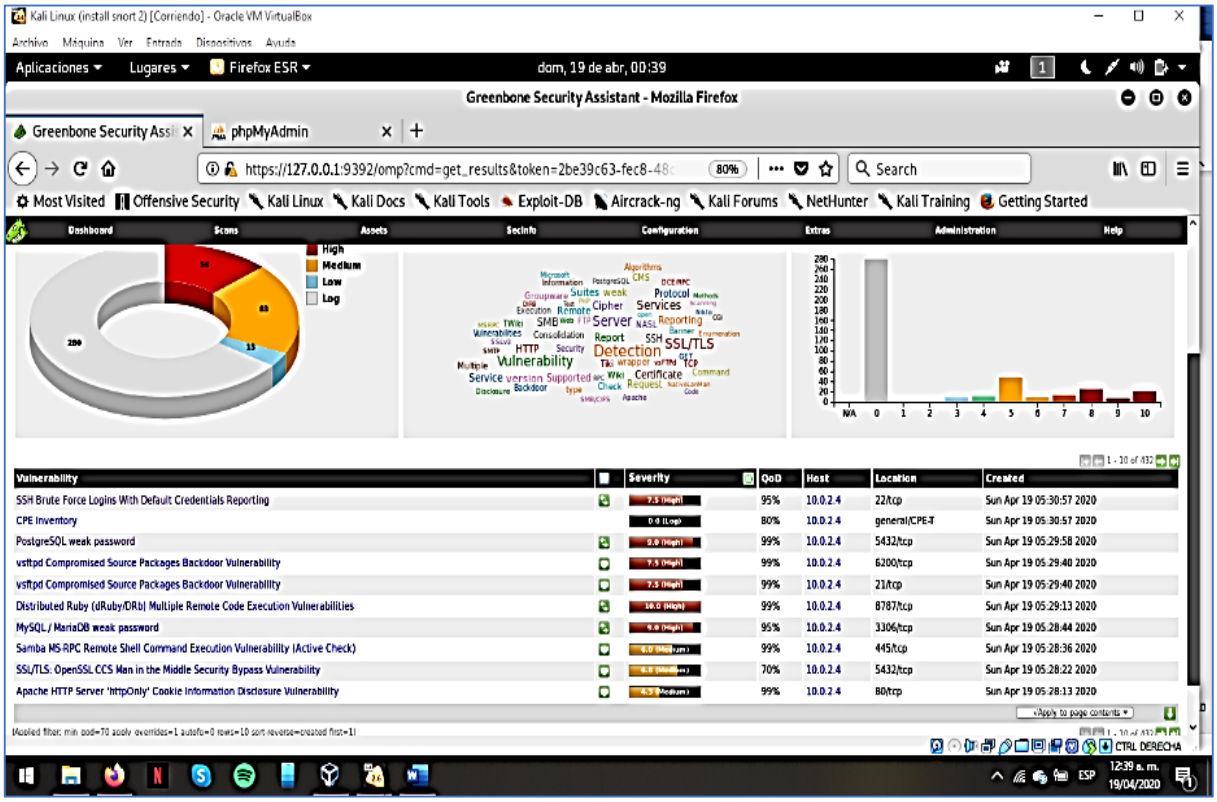
Figura 32 Escaneo OPENVAS Configurado



Fuente: William Salcedo Rodríguez

Finalmente, al terminar el 100% del escáner, en el apartado de resultados se obtienen todas las vulnerabilidades encontradas en la máquina Metasploitable, también se sugiere que Exploit se deben usar para atacar estas vulnerabilidades y algunos complementos o repositorios que pueden corregir estas vulnerabilidades. En la figura 33 se muestra el listado de vulnerabilidades encontradas.

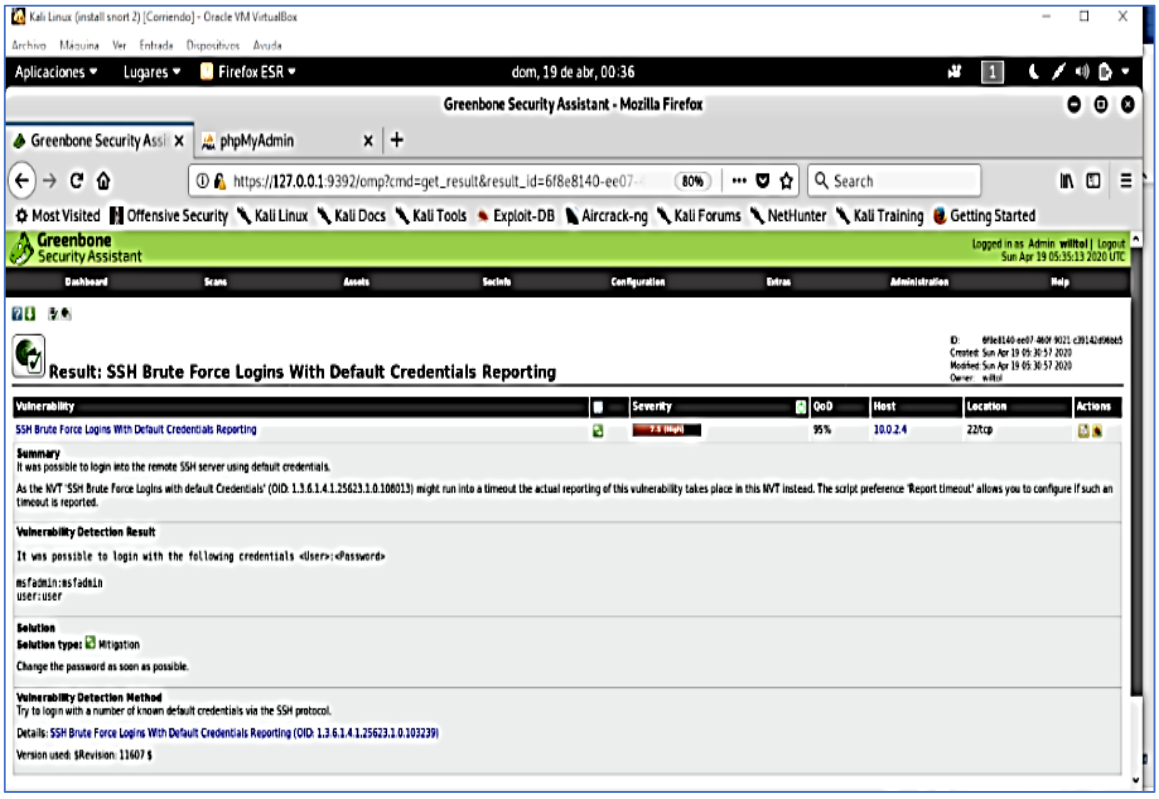
Figura 33 Resultados escaneo de vulnerabilidades OPENVAS



Fuente: William Salcedo Rodríguez

Entre los resultados obtenidos se analizarán los que pueden indicar que vulnerabilidades se pueden atacar para lograr acceder al servidor Metasploitable, de esta manera lograr materializar los ataques de tipo Defacement, en la figura 34 se muestra la vulnerabilidad de credenciales de acceso por medio del servicio SSH.

Figura 34 Vulnerabilidades credenciales por default SSH



Fuente: William Salcedo Rodríguez

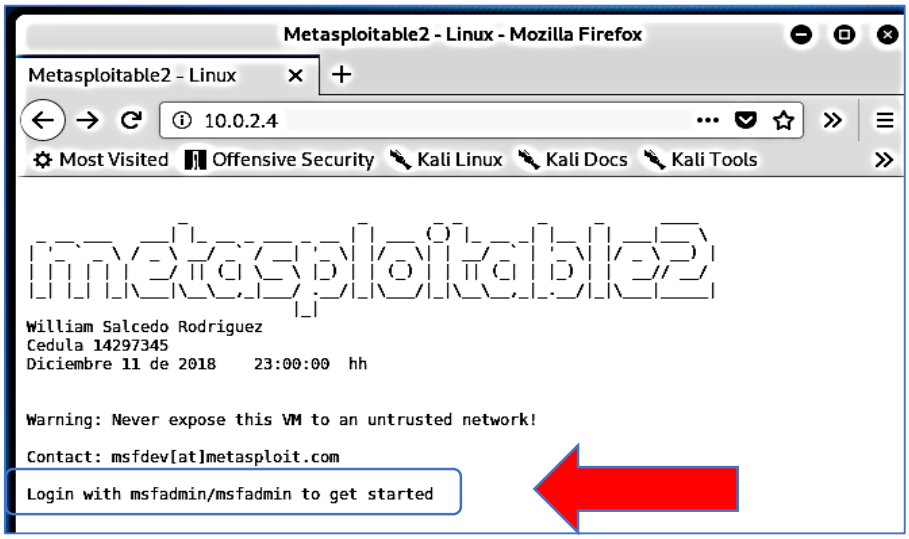
Este resultado revela que es posible conectarse por fuerza bruta a través del protocolo SSH, debido a que las credenciales por defecto están establecidas, lo que es una grave falla de seguridad, en este caso las credenciales por defecto pueden ser:

user:user

msfadmin: msfadmin

En la figura 35 se evidencia la dirección IP del servidor Metasploitable a través del navegador web, el cual revela el usuario y contraseña de acceso por default.

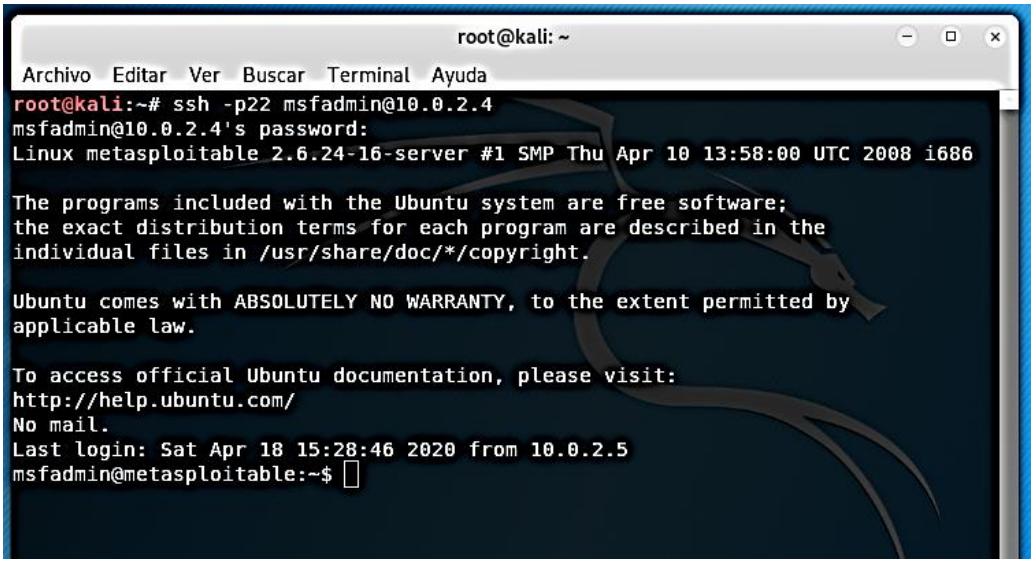
Figura 35 Página principal servidor Metasploitable



Fuente: William Salcedo Rodríguez

Se intenta hacer la conexión de acceso remoto al servidor ya que se tienen todas las variables para establecer la conexión, para tal prueba desde un terminal en el servidor Kali Linux se ingresa la siguiente instrucción: *ssh -p22 msfadmin@10.0.2.4*, la figura 36 muestra la conexión exitosa con el servidor Metasploitable.

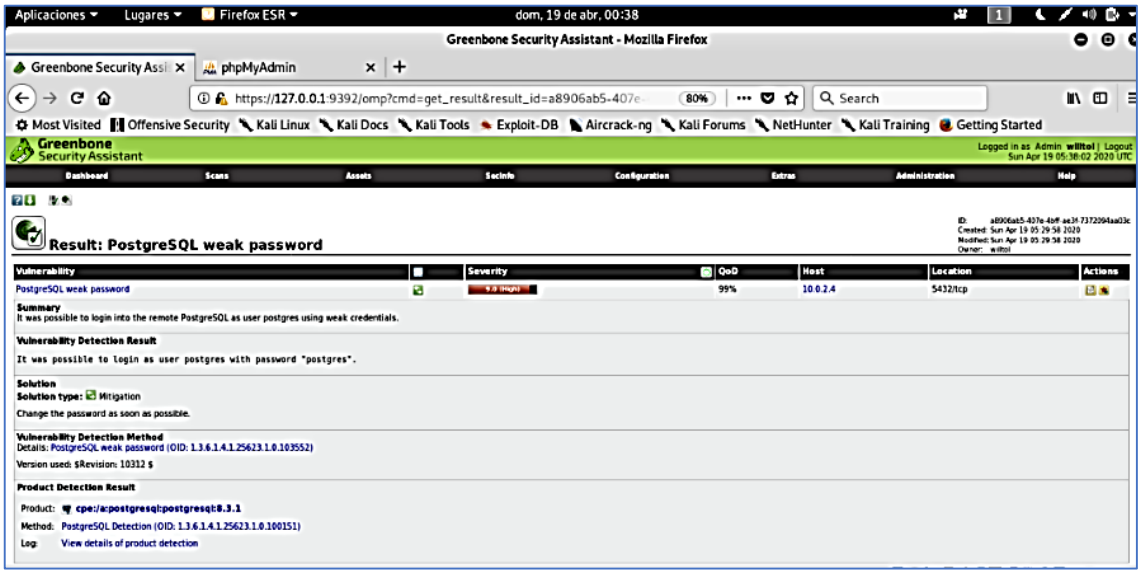
Figura 36 Conexión SSH a Servidor Metaspoitable



Fuente: William Salcedo Rodríguez

En la figura 37 se muestra la vulnerabilidad encontrada sobre el sistema gestor de base de datos PostgreSQL, el cual sugiere una contraseña por default para acceder.

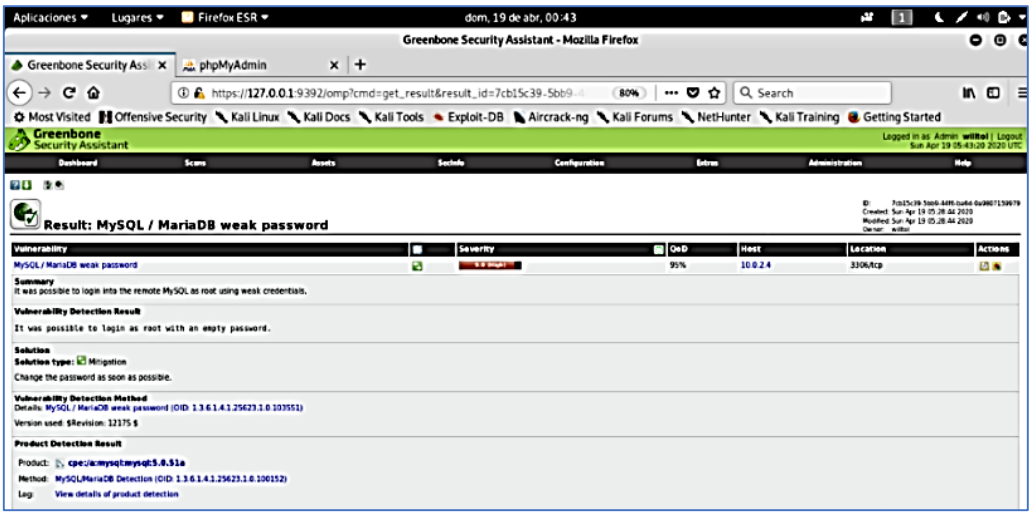
Figura 37 Vulnerabilidad Postgres Default Password



Fuente: William Salcedo Rodríguez

Este resultado revela que existe vulnerabilidad en el gestor de base de datos PostgreSQL, el cual puede tener por defecto el usuario postgres y contraseña postgres, esta es una gran falla de seguridad debido a que, si un atacante logra ingresar al gestor de base de datos PostgreSQL con estas credenciales, podría acceder a la base de datos y la información allí alojada. En la figura 38 se puede ver la vulnerabilidad presente en MySQL.

Figura 38 Vulnerabilidad MySQL Password



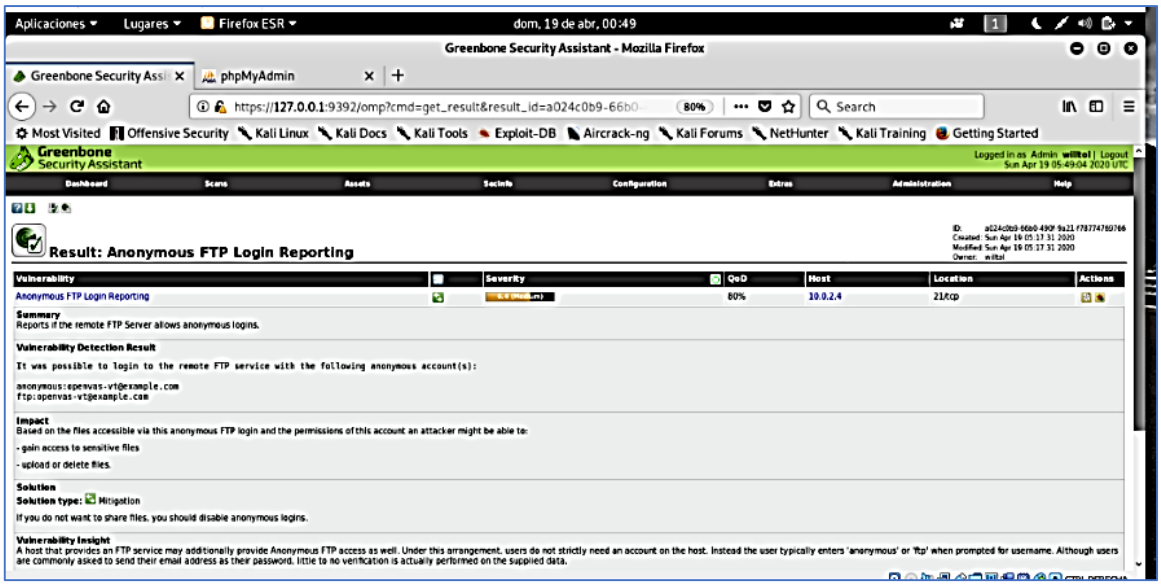
Fuente: William Salcedo Rodríguez

Este resultado revela que existen vulnerabilidades en la seguridad de acceso a MySQL, en la cual puede ser posible acceder a MySQL de manera remota usando las siguientes credenciales, en la figura 39 se evidencia la vulnerabilidad presente en el servicio FTP

Usuario: root

Password: (Empty) Es decir se deja en blanco el espacio contraseña.

Figura 39 Vulnerabilidad FTP



Fuente: William Salcedo Rodríguez

Este resultado evidencia una vulnerabilidad presente en el servicio ftp, al cual es posible acceder de manera remota con las siguientes cuentas:

anonymous: OPENVAS-vt@example.com

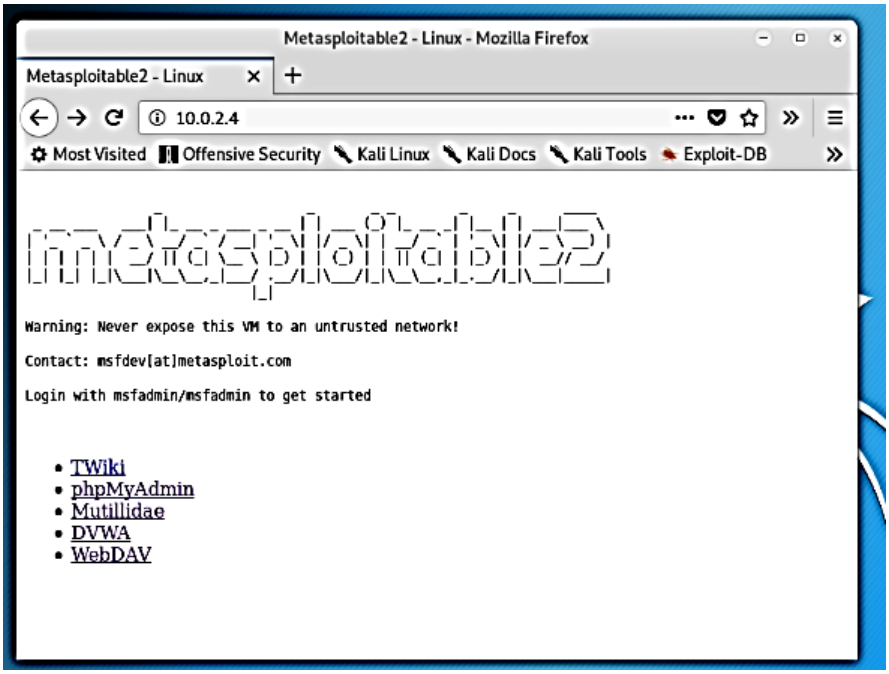
ftp: OPENVAS-vt@example.com

De esta manera se identifican vulnerabilidades con las herramientas de auditoria informática, tales como puertas traseras que permiten una conexión a través del protocolo SSH ya que también fue posible identificar las credenciales de acceso por defecto al servidor Metasploitable

9.6 Simulación de Ataque Tipo Defacement

En esta fase es simulado el ataque de tipo DEFACEMENT, realizado sobre la entidad estatal en su sede principal, este ataque es simulado utilizando el software de auditoria informática Kali Linux como la máquina atacante, y la máquina con sistema Linux Metasploitable como la víctima. En la figura 40 se muestra la página principal del servidor Metasploitable.

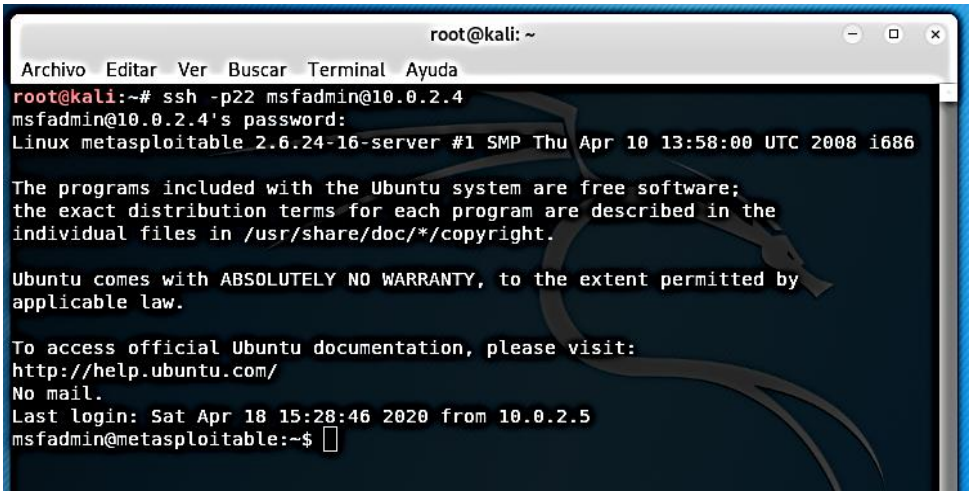
Figura 40 Página Principal Servidor Metasploitable



Fuente: William Salcedo Rodríguez

El objetivo del ataque es desfigurar la apariencia de su página principal accediendo ilícitamente desde el servidor Kali Linux. Desde el servidor Kali Linux se ejecuta una terminal y se accede al servidor Metaspoitable de manera remota por medio del servicio SSH puerto 22/TCP, utilizando las siguientes credenciales, Usuario: msfadmin contraseña: msfadmin, tal cual como se evidencia en la figura 41.

Figura 41 Conexión SSH a servidor Metasploitable

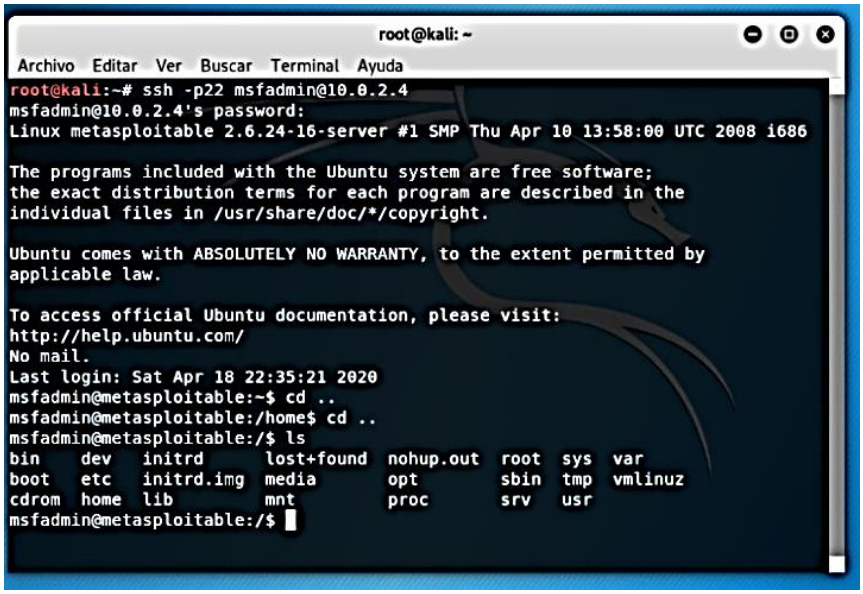


Fuente: William Salcedo Rodríguez

Al estar conectados de manera remota en el servidor Metasploitable, se debe de ubicar la ruta en la cual está alojada la página principal del servidor.

Para acceder, se ubica en la raíz del sistema ingresando el comando *cd* ..hasta quedar en la raíz, después se ingresa el comando *ls* para listar los directorios de la raíz del sistema, la figura 42 muestra los directorios presentes en la raíz del sistema.

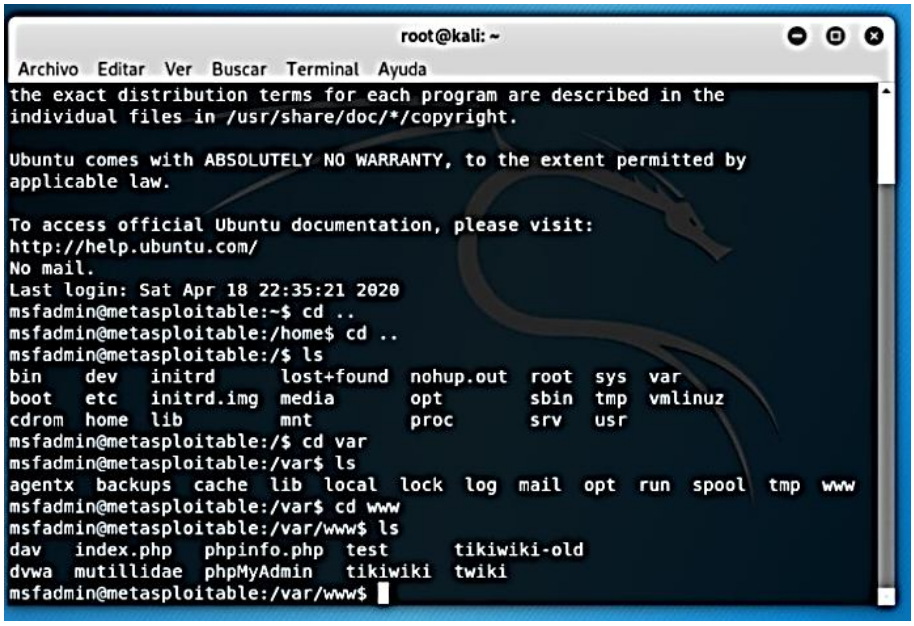
Figura 42 Comando ls listar directorios Raíz



Fuente: William Salcedo Rodríguez

Se accede al directorio var ingresando el comando *cd var*, y listar de nuevo, aparece un directorio www al cual se accede ingresando el comando *cd www* y listar de nuevo con el comando *ls*. En la figura 43 se listan los archivos del directorio VAR/WWW

Figura 43 Comando ls listar directorios www

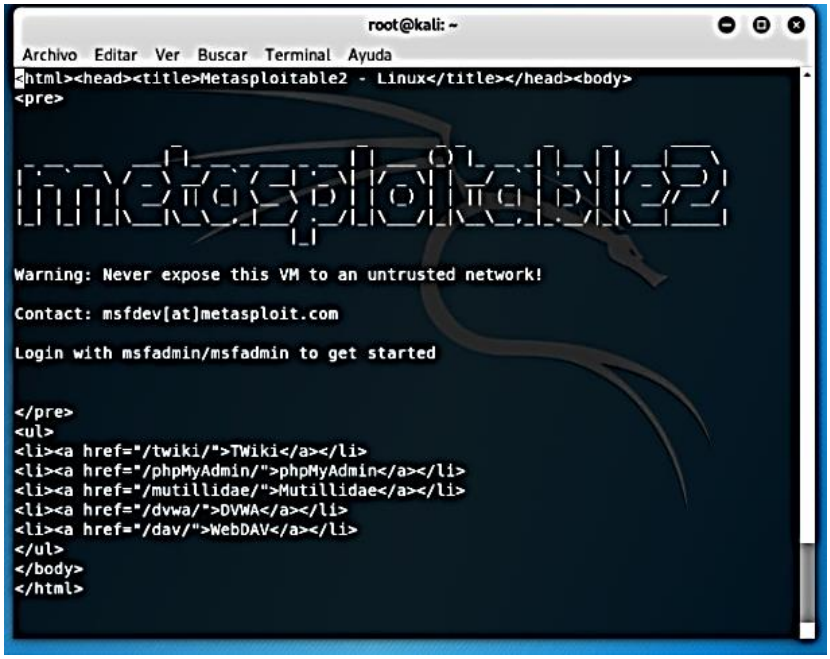


Fuente: William Salcedo Rodríguez

Al listar aparecen los archivos del sitio web principal del servidor Metasploitable, entre estos el archivo index.php, el cual es la página principal del servidor y el objetivo del ataque.

Para modificar este sitio web se accede con un editor de comando, en este caso se hizo uso del editor vi, ingresando el comando *sudo vi index.php*, la figura 44 muestra el uso del editor vi.

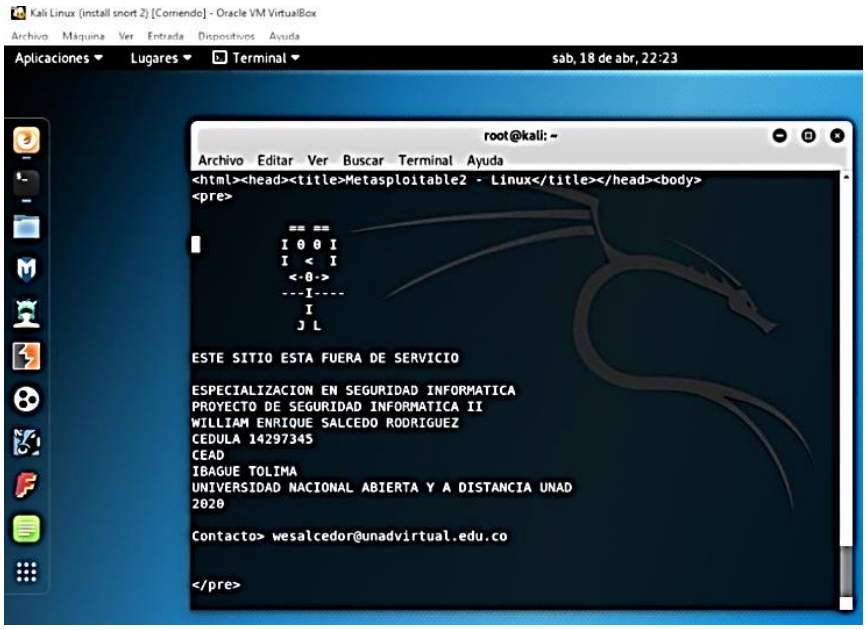
Figura 44 Comando vi editar index.php



Fuente: William Salcedo Rodríguez

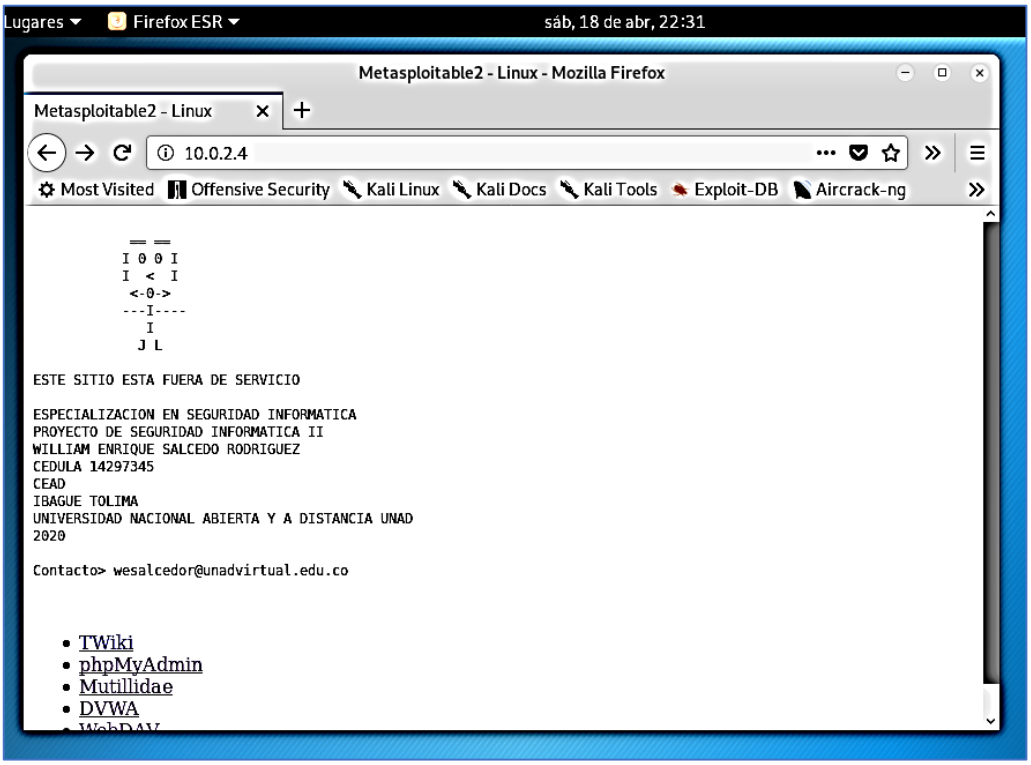
En la figura 45 se edito el sitio, en este caso, se elimina parte del contenido y se agregan mis datos de contacto como evidencia de que los cambios registrados son de mi autoría.

Figura 45 Edición de index.php comando VI



Fuente: William Salcedo Rodríguez

Figura 46 Ataque Defacement Materializado



Fuente: William Salcedo Rodríguez

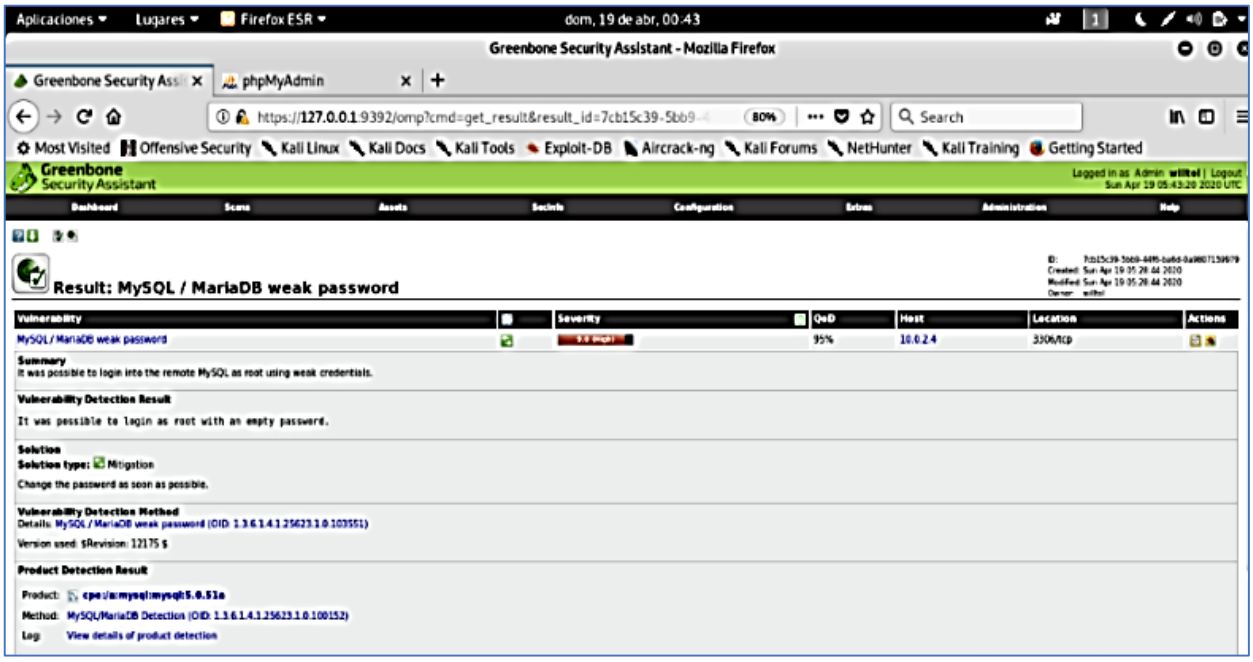
Una vez ha sido editado el archivo index.php, se guardan los cambios y se accede al navegador web ingresando la dirección del servidor Metasploitable 10.0.2.4, en la cual debe de mostrar la página principal del servidor con el DEFACEMENT que se ha realizado sobre este, la figura 46 evidencia que la página principal del servidor web ha sido alterada.

De esta manera se materializo el ataque de tipo Defacement, el cual en un ambiente real puede afectar la disponibilidad de la informacion en un servidor web.

9.7 Simulación de Ataque Tipo Ransomware

En esta fase es simulado el ataque de tipo RANSOMWARE, el cual fue realizado sobre la entidad estatal en su segunda sede, este ataque es simulado utilizando el software de auditoria informática Kali Linux como la máquina atacante y la máquina con sistema Linux Metasploitable, como la víctima. Para realizar este ataque se ataca la vulnerabilidad encontrada sobre MySQL, tal cual como se evidencio en la figura 47.

Figura 47 Vulnerabilidad MySQL

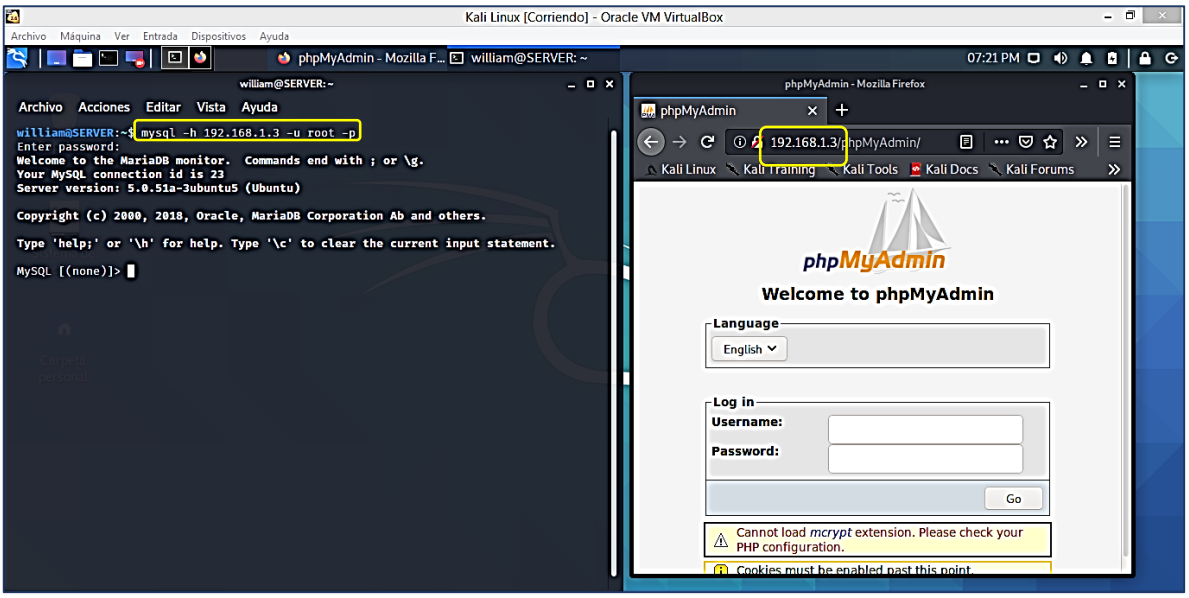


Fuente: William Salcedo Rodríguez

En esta evidencia se refleja una vulnerabilidad sobre MySQL en la cual se puede obtener acceso remoto con usuario: root y contraseña en blanco. Desde una terminal de Kali Linux se ingresa el siguiente comando: *mysql -h 192.168.1.3 -u root -p.*

La figura 48 evidencia el acceso remoto a MySQL.

Figura 48 Acceso remoto MySQL

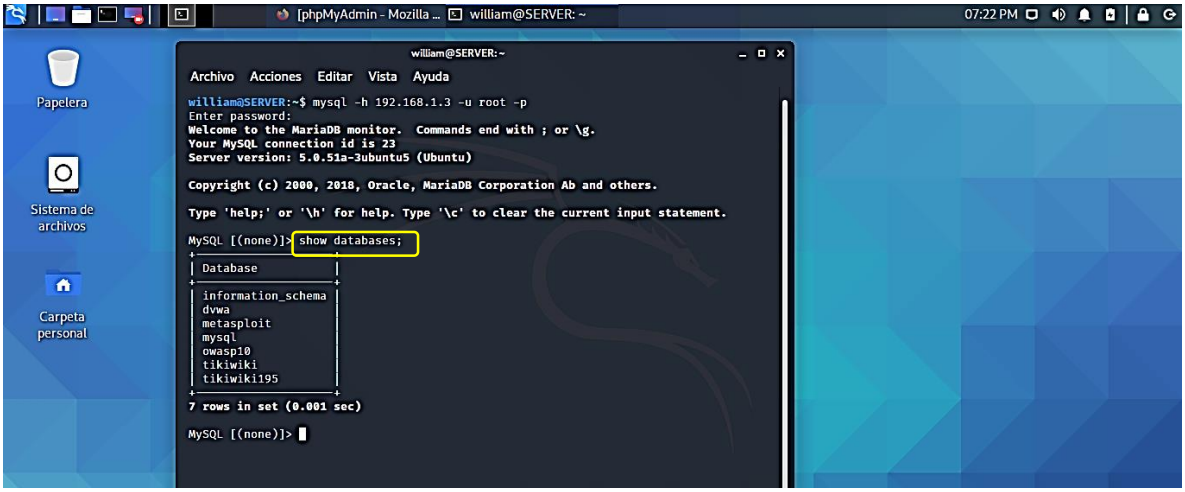


Fuente: William Salcedo Rodríguez

Una vez se ha ingresado a MySQL, es posible navegar por la línea de comandos en MySQL hasta encontrar la base de datos que contenga la información que se quiere secuestrar, como parte del ataque de tipo RANSOMWARE que se quiere materializar, en la figura 49 se listan las bases de datos existentes con el comando:

show databases;

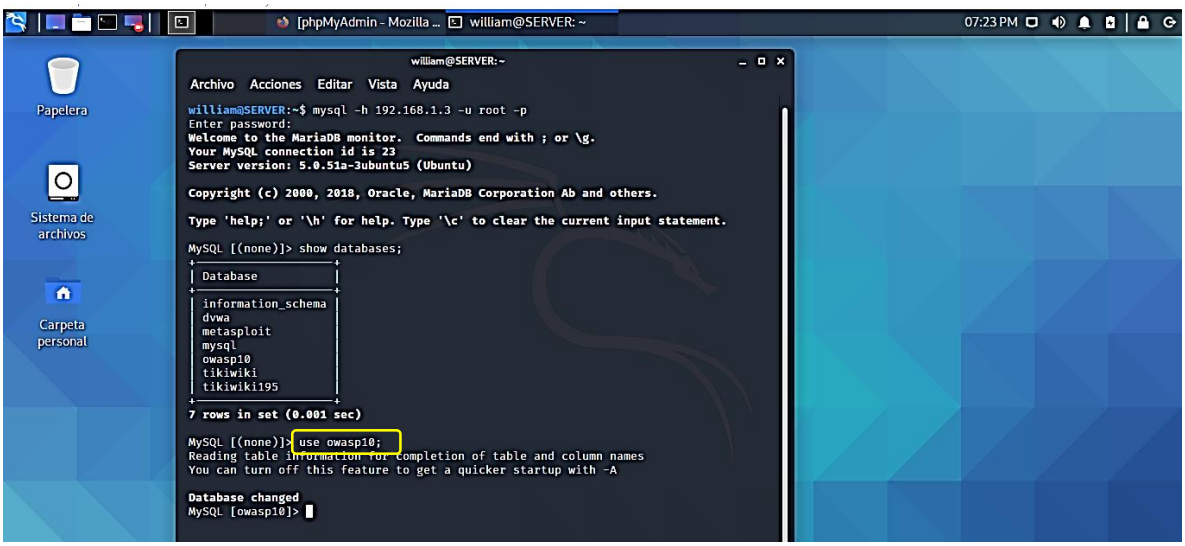
Figura 49 Comando MySql > "show databases;"



Fuente: William Salcedo Rodríguez

Una vez listadas las bases de datos, se debe seleccionar la base de datos que es objetivo del ataque, en la figura 50 se evidencia el listado de las bases de datos, para ingresar a la base de datos owasp10 se ingresa el siguiente comando: *use owasp10;*

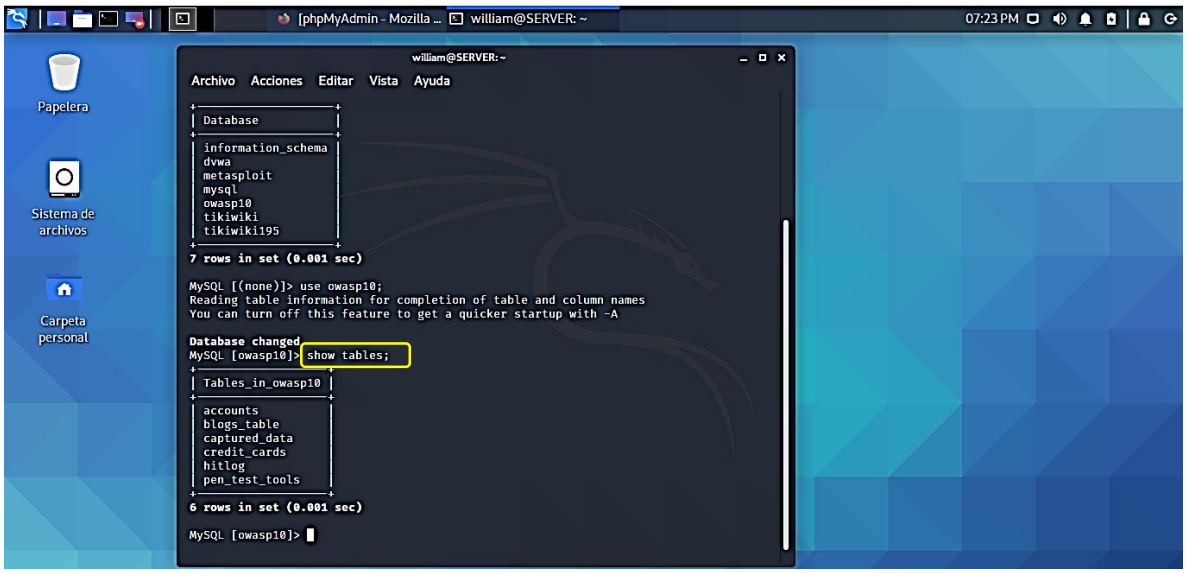
Figura 50 Comando Mysql > "use databases;"



Fuente: William Salcedo Rodríguez

En la figura 51 se ingresa el comando *Show tables;* para mostrar las tablas de la base de datos owasp10:

Figura 51 Comando Mysql > "show tables;"

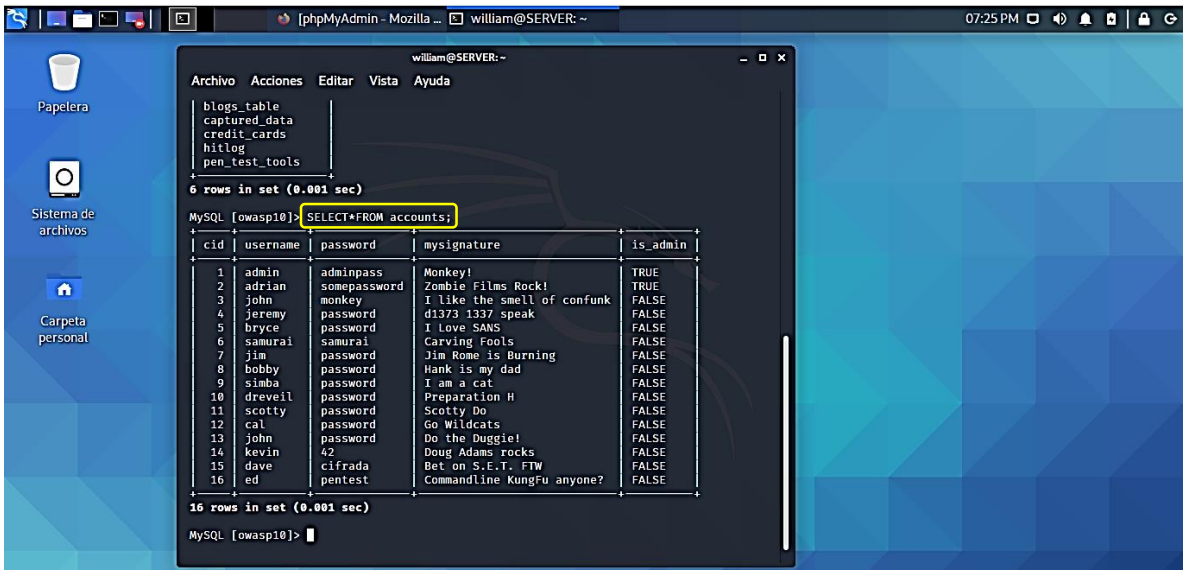


Fuente: William Salcedo Rodríguez

En este punto ya se tiene control y acceso sobre la base de datos, entre las tablas que se pueden visualizar, se va a examinar la tabla accounts ingresando el siguiente comando respectivamente:

SELECT * FROM accounts;

Figura 52 Comando MySQL > "SELECT * FROM accounts;"



Fuente: William Salcedo Rodríguez

Hasta este punto hemos accedido al servidor Metasploitable y tenemos acceso remoto las bases de datos, ahora podemos materializar el ataque tipo Ransomware, recordemos que existen dos tipos de ataques Ransomware, de bloqueo y cifrado.

El Ransomware de tipo bloqueo como su nombre lo indica bloquea a la victima el acceso al dispositivo para que no pueda utilizarlo para después cobrar un rescate por desbloquear el dispositivo.

El Ransomware de tipo cifrado como su nombre lo indica cifra informacion valiosa para la victima para que no puede acceder a esta informacion, en este caso el atacante tiene una llave o contraseña con la cual encripto la informacion y cobra un rescate por esta llave para que la victima pueda acceder de nuevo a su informacion.

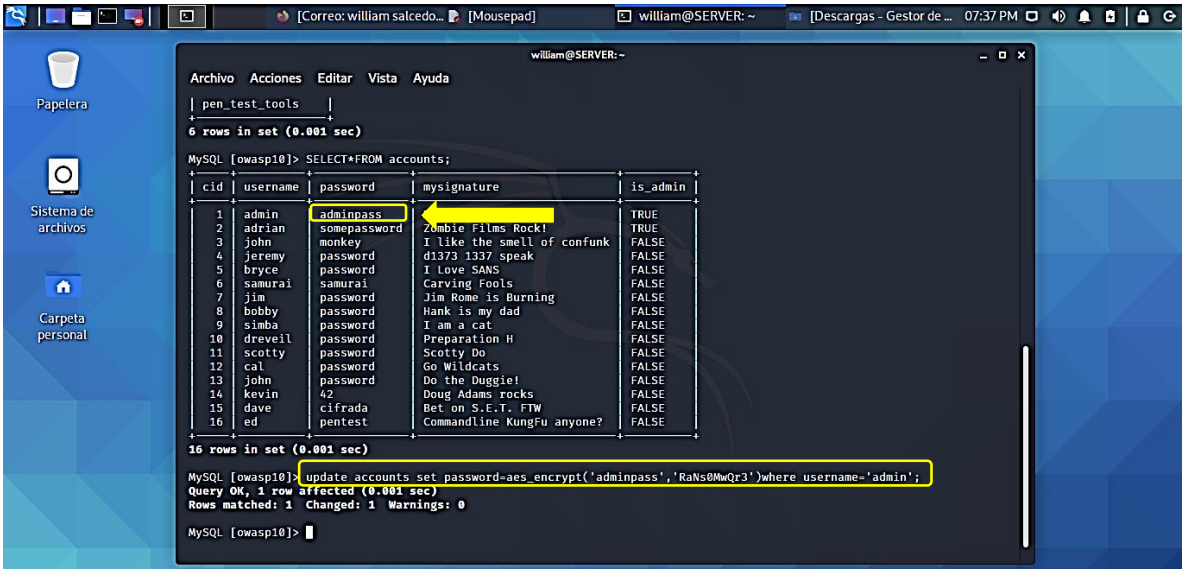
En este caso se hizo uso del tipo de ataque Ransomware de cifrado y precisamente ciframos un registro de la base de datos, específicamente se realizo cifrado sobre la contraseña principal del username “admin” la cual esta alojada en la tabla accounts de la base de datos owasp10

Para llevar a cabo este proceso ingresamos la siguiente instrucción:

update accounts set password=aes_encrypt('adminpass','RaNs0MwQr3')where username='admin';

tal cual como lo indica la figura 53

Figura 53. Instrucción encriptado aes_encrypt

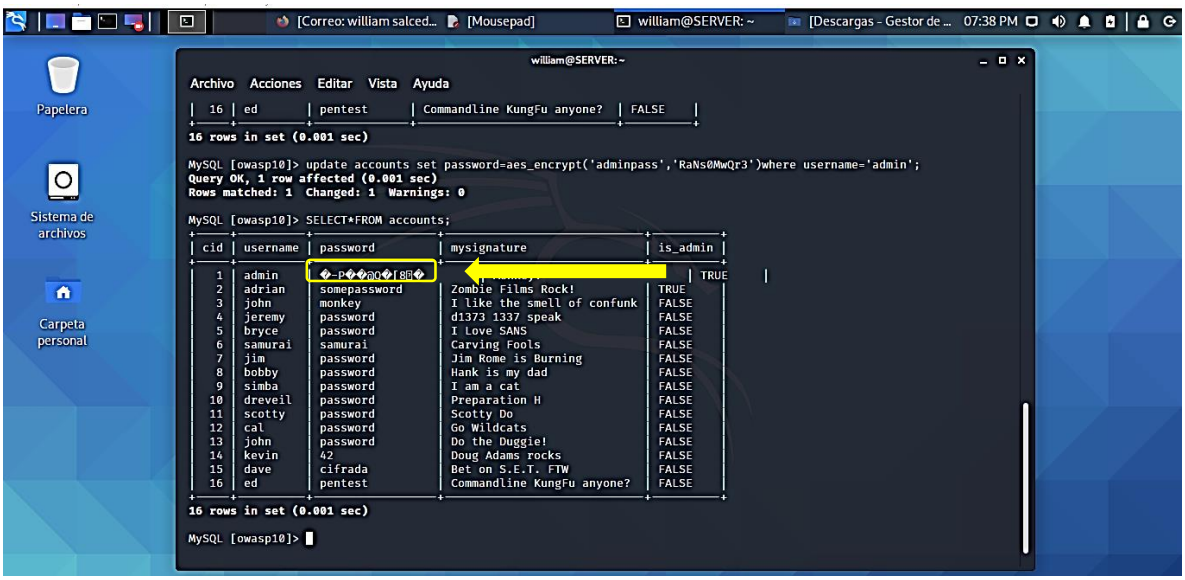


Fuente: William Salcedo Rodríguez

En esta instrucción le indicamos que actulice el valor de la columna password relacionado con el username admin, pero lo ciframos haciendo uso de la instrucción aes_encrypt seguido de el registro que esta en ese campo “adminpass” mas la contraseña con la cual

queda encriptado “RaNs0MwQr3” de esta forma al ejecutar la instrucción este valor quedara cifrado tal cual como lo refleja la figura 54 al consultar de nuevo la tabla accounts con la instrucción: *SELECT*FROM accounts;*

Figura 54. Registro cifrado



Fuente: William Salcedo Rodríguez

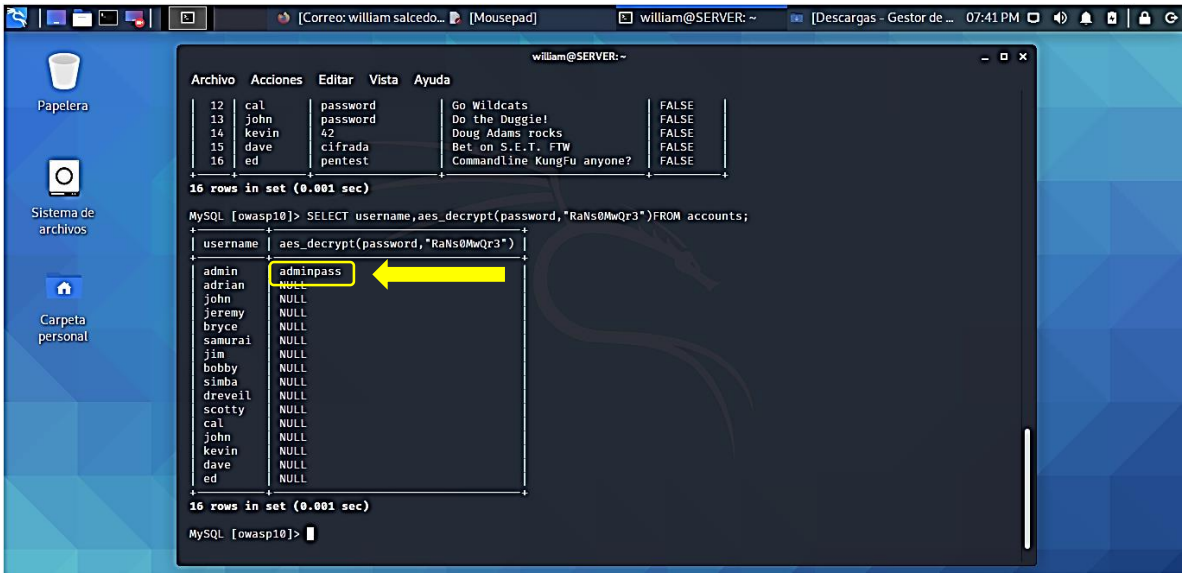
Podemos evidenciar que el registro del campo password asociado al username admin aparece con una codificación ilegible ya que ha sido cifrado, para que la victima pueda visualizar de nuevo este registro es necesario que tenga la contraseña o llave de encriptación, de esta manera se ha materializado el ataque Ransomware de tipo cifrado, en este caso se notifica a la victima que ha sido objeto de un ataque Ransomware y si desea obtener la informacion cifrada debe de pagar una recompensa.

Si la victima tiene la contraseña o llave con la cual encriptaron este registro, puede visualizarlo de nuevo con la siguiente instrucción:

SELECT username,aes_decrypt(password,"RaNs0MwQr3")FROM accounts;

Tal cual como lo evidencia la figura 55.

Figura 55. Instrucción desencriptado aes_decrypt



Fuente: William Salcedo Rodríguez

Como pueden ver la instrucción nos muestra en pantalla solamente los registros de la columna username cuyo password ha sido encriptada con la clave: RaNs0MwQr3, en este caso el valor: adminpass que corresponde a la contraseña de la cuenta admin por la cual se solicito rescate.

10 IDENTIFICACION DE VULNERABILIDADES Y DISEÑO DE CONTROLES SOBRE LA ENTIDAD ESTATAL

Para el desarrollo de la presente etapa se hizo uso de la metodología MAGERIT, esta metodología es muy útil, debido a que nos permite realizar de manera ordenada las siguientes fases:

Tabla 1 Fases de la metodología MAGERIT

SECUENCIA	PROCESOS
Fase 1	Identificación y valoración de activos
Fase 2	Identificación y valoración de amenazas y vulnerabilidades
Fase 3	Diseño de salvaguardas

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

10.1 FASE 1. IDENTIFICACIÓN DE ACTIVOS

En esta fase se identificaron los activos principales de la entidad estatal en sus sedes principal y secundaria. La nomenclatura de los activos se basa en la metodología MAGERIT, clasificando los activos de la siguiente manera:

[D] - Datos/Informacion

[S] - Inventario de servicios

[SW] - Aplicaciones informáticas – Software

[HW] - Equipos informáticos

[COM] - Redes de comunicaciones

[MEDIA] - Soportes de Información. Electrónico/No Electrónico

[AUX] - Equipamiento Auxiliar:

[L] - Instalaciones

[P] – Personal.

Tabla 2.[D] Datos/Información

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[files]	Ficheros de datos	[Archivo Informacion entidad]	Archivos con la informacion propia de la entidad estatal
		[Archivo Datos personales]	Informacion personal de ciudadanos alojada en servidores de la entidad.
[backup]	Copias de respaldo	[Archivo Copias de Respaldo]	Archivo de copias de seguridad de la Información
[password]	Credenciales	[Contraseñas Empleados]	Contraseñas de acceso de empleados
[source]	Código fuente	[Código fuente aplicativos entidad estatal	Código fuente portal web de la entidad estatal

Fuente: William Salcedo Rodríguez

Tabla 3 [S] Servicios

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[int]	Interno (usuarios y medios de la propia organización)	[Servicio Interno]	Servicio administración y soporte de sistemas de información
			Servicio de administración y contratación de servicios
			Servicio de administración servidores, máquinas virtuales, dispositivos de la entidad.
			Servicio de desarrollo y mantenimiento plataformas
[www]	World Wide web	[Servicio Internet]	Servicio de internet
[email]	Correo electrónico	[Servicio Correo]	Manejo de correos electrónicos
[file]	Almacenamiento de ficheros	[Bases de datos]	Servicio de almacenamiento de información en los servidores de bases de datos.

Fuente: William Salcedo Rodríguez

Tabla 4 Aplicaciones informáticas

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[browser]	Navegador Web	[Navegadores]	Navegadores Google Chrome y Mozilla Firefox
[app]	Servidor de aplicaciones	[Server Aplicación]	Servidores de Aplicaciones
[web server]	Plataforma Web	[Server web]	Plataforma Web
[file]	servidor de ficheros	[Server Ficheros]	Servidor de Ficheros
[dbms]	Sistema de gestión de bases de datos	[SG Base Datos]	SQL server, Oracle, PostgreSQL, MySQL
[Office]	Ofimática	[Office]	Office: 2013 y 2016
[av]	Antivirus	[Antivirus]	McAfee® Total Protection
[os]	Sistema operativo	[OS Win]	Sistema operativo Windows 8 y Windows 10.
			Sistema operativo Linux
[hipervisor]	Gestor de máquinas virtuales	[máquinas virtuales]	Máquina virtual VirtualBox
[backup]	Sistema de backup	[backup]	Sistema de backup en el servidor

Fuente: William Salcedo Rodríguez

Tabla 5. [HW] Hardware

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[host]	Grandes equipos (host)	[Servicio Aplicaciones]	Servidor Aplicaciones
		[Servicio Web]	Servidor Web
		[Servicio Data Base]	Servidor para copias de seguridad
[mid]	Equipos medios	[PC Equipos de Escritorio]	Computadores de escritorio
[pc]	Informática personal	[PC portátiles]	Computadores Portátiles
[vhost]	Equipos virtuales (máquinas virtuales)	[máquinas virtuales Equipos virtual]	Máquinas virtuales con servicios internos y externos
[print]	Medios de impresión	[Equipamiento Impresoras]	Impresoras
[scan]	Escáner	[Servicio Scan]	Escáner
[switch]	conmutadores	[switch conmutadores]	conmutadores
[router]	Enrutadores	[Router enrutadores]	Dispositivos Cisco
[other]	rack	[rack]	rack

Fuente: William Salcedo Rodríguez

Tabla 6. [COM] Redes de Comunicaciones

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[wifi]	Wifi	[Wifi]	Red Inalámbrica
[LAN]	Red local	[Red Local]	Red local
[Internet]	Internet	[Internet]	Internet
[Intranet]	Intranet	[intranet]	Intranet

Fuente: William Salcedo Rodríguez

Tabla 7. [MEDIA] Soportes de Información

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[disk]	Discos	[Almacenamiento CD]	Almacenamientos en Disco Duro
[USB]	Memorias USB	[Almacenamiento Memorias]	Almacenamiento en Memorias
[dvd]	DVD	[A_DVD]	Almacenamiento en DVD
[printed]	Material impreso	[Car]	Cajas con sus carpetas debidamente archivadas (Folios, archivos históricos, hojas de vida.)
		[archivadores]	Archivadores con sus carpetas debidamente archivadas
		[Informes]	Reportes de informes impresos
		[varios]	Carpetas varias

Fuente: William Salcedo Rodríguez

Tabla 8. [AUX] Equipamiento auxiliar

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[ups]	Sistemas de Alimentación ininterrumpida	[Ups sala de comunicaciones]	UPS sala de comunicaciones
[Ac]	Equipos de Climatización	[Equipos Cli]	Aire Acondicionado en la sala de Comunicaciones
[wire]	Cable Eléctrico	[Cable Eléctrico]	Cable Eléctrico
[fiber]	Fibra Óptica	[Fibra óptica]	Transmisión de comunicación
[suplly]	Suministros Esenciales	[Suministro Esenciales]	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.

Fuente: William Salcedo Rodríguez

Tabla 9. [L] Instalaciones

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[building]	Edificio	[Edificio entidad estatal sede principal]	Entidad estatal sede principal
[building]	Edificio	[Central de datos entidad sede principal]	Oficina Gestión informática
[building]	Edificio	[Edificio entidad estatal sede secundaria]	Entidad estatal sede secundaria
[building]	Edificio	[Central de datos entidad sede secundaria]	Oficina Gestión informática

Fuente: William Salcedo Rodríguez

Tabla 10. [P] Personal

CÓDIGO CLASES DE ACTIVO MAGERIT	NOMBRE DE LA CLASE DE ACTIVO MAGERIT	CÓDIGO ACTIVO DE LA ENTIDAD	NOMBRE ACTIVO DE LA ENTIDAD
[ui]	Usuarios internos	[personal interno]	Funcionarios públicos
			Contratistas

Fuente: William Salcedo Rodríguez

10.1.1 Criterios de valoración de activos

Los activos de la organización tienen un valor, dependiendo de qué tan indispensables son y de que tan crítico puede ser para la organización si este activo presenta falla o ausencia permanente. En la siguiente tabla se indican los niveles de criticidad o importancia y que tan grave es su impacto sobre la organización.

Tabla 11. Criterios de valoración de activos

	VALOR	CRITERIO
5	Muy Alto	Daño muy grave
4	Alto	Daño grave
3	Medio	Daño importante
2	Bajo	Daño menor
1	Muy Bajo	Irrelevante a efectos prácticos

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

10.1.2 Dimensiones de valoración de activos

Así como los activos tienen unos criterios de valoración, también tienen unas facetas o dimensiones, que permiten realizar análisis de riesgos sobre esta dimensión en particular, el valor que se dé sobre el activo en una dimensión refleja el daño que implica sobre la organización si el activo se ve afectado en esta dimensión. Las principales dimensiones de un activo son las siguientes:

Tabla 12. Dimensiones de valoración de un activo

DIMENSIONES	DESCRIPCIÓN	NIVELES	DESCRIPCION
[D] Disponibilidad	Propiedad en la que el activo puede ser accedido por los actores o entidades autorizadas, en el momento requerido.	Alto	Afecta gravemente a la organización, disponibilidad 100%
		Medio	El nivel de afectación es aceptable, disponibilidad 75%
		Bajo	No genera grandes daños sobre la organización, disponibilidad 25%
[I] Integridad de los datos	Propiedad en la que el activo de informacion no se ve modificado por personal no autorizado.	Alto	Informacion sensible que afecta gravemente a la organización.
		Medio	Informacion de tipo privado y público que genera un daño aceptable sobre la organización.
		Bajo	Informacion de carácter público, su alteración no genera daños sobre la organización.
[C] Confidencialidad	Propiedad en la que la informacion no se pone a disposición de entidades o procesos no autorizados.	Alto	Activo sensible de acceso privado, afecta gravemente a la organización.
		Medio	Activo de acceso a personal autorizado con restricciones, puede generar algunos daños sobre la organización.
		Bajo	Activo de carácter público, genera poca afectación sobre la organización.

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

A continuación, se hizo una clasificación de los principales activos según estos niveles de criticidad y dimensiones.

Tabla 13. Relación valoración de principales activos

ACTIVO	TIPO DE ACTIVO	DIMENSIONES DEL ACTIVO			VALORACIÓN DEL ACTIVO		RESPONSABLE PRINCIPAL
		[C]	[I]	[D]	NIVEL	VALOR	
Código fuente del portal web de la entidad estatal	D	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Archivo de copias de seguridad de la Información	D	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Contraseñas de acceso de empleados	D	Alto	Medio	Bajo	Medio	3	Oficina Gestión informática
Correo electrónico Institucional	S	Medio	Medio	Bajo	Bajo	2	Oficina Gestión informática
Servicio de administración servidores, máquinas virtuales y dispositivos.	S	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Servicio de desarrollo y mantenimiento plataformas de la entidad	S	Medio	Medio	Alta	Alto	4	Oficina Gestión informática
Sistema de Backups en el servidor	SW	Alto	Alto	Medio	Alto	4	Oficina Gestión informática
Servidores de Aplicaciones	SW	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Sistema de gestión de bases de datos	SW	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Servidor web	HW	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Servidor Aplicaciones	HW	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática
Máquinas virtuales con servicios internos y externos	HW	Alto	Alto	Alto	Muy Alto	5	Oficina Gestión informática

Continuacion Tabla 13

ACTIVO	TIPO DE ACTIVO	DIMENSIONES DEL ACTIVO			VALORACIÓN DEL ACTIVO		RESPONSABLE PRINCIPAL
		[C]	[I]	[D]	NIVEL	VALOR	
Computadores de escritorio y portátiles	HW	Medio	Medio	Bajo	Bajo	2	Oficina Gestión informática
Red local	COM	Medio	Medio	Alto	Medio	3	Oficina Gestión informática
Almacenamientos en Disco Duro	MEDIA	Alto	Alto	Medio	Alto	4	Oficina Gestión informática
UPS sala de comunicaciones	AUX	Bajo	Bajo	Alto	Alto	4	Oficina Gestión informática
Oficina Gestión informática sede principal	L	Alto	Medio	Alto	Muy Alto	5	Oficina Gestión informática
Oficina Gestión informática sede secundaria	L	Alto	Medio	Alto	Muy Alto	5	Oficina Gestión informática
Personal Interno	P	Alto	Medio	Medio	Alto	4	Oficina Gestión Humana

Fuente: William Salcedo Rodríguez

10.2 FASE 2. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

En la siguiente fase se identifican las principales amenazas sobre los activos, según la clasificación del método de análisis y gestión de riesgo MAGERIT. Entre las principales amenazas que se pueden presentar, está la siguiente clasificación.

Tabla 14. Clasificación de amenazas

IDENTIFICACIÓN DE LAS AMENAZAS	
[N]	Desastres naturales
[I]	De Origen Industrial
[E]	Errores y fallos no intencionados
[A]	Ataques intencionados

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Las amenazas sobre los activos tienen un impacto sobre la organización y presentan cierta frecuencia de acción, a continuación, se determinan las escalas usadas para analizar las amenazas sobre cada activo.

Tabla 15. Rango de frecuencia de amenazas

VULNERABILIDAD	RANGO	VALOR
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada semana	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Tabla 16.Rango de impacto

SIGLAS	IMPACTO	VALOR CUANTITATIVO
MA	Muy alto	100%
A	Alto	75%
M	Medio	50%
B	Bajo	20%
MB	Muy bajo	5%

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

A continuación, se hizo el análisis sobre los principales activos, según las principales amenazas que los pueden atacar, teniendo en cuenta sus 3 dimensiones, la frecuencia de acción y el grado de impacto sobre la organización.

Tabla 17. Relación de amenazas por desastres naturales sobre activos

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %		
			[C]	[I]	[D]
[N.1] FUEGO	[HW_COMPUTADORES DE ESCRITORIO]	5			MA
	[HW_COMPUTADORES PORTÁTIL]	5			MA
	[HW_IMPRESORAS]	5			MA
	[HW_ESCANER]	5			MA
	[HW_SERVIDOR APLICACIONES]	5			MA
	[HW_SERVIDOR WEB]	5			MA
	[AUX_UPS SALA DE COMUNICACIONES]	5			A
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5			A
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5			A
[N.2] DAÑOS POR AGUA	[HW_COMPUTADORES DE ESCRITORIO]	5			M
	[HW_COMPUTADORES PORTÁTIL]	5			MA
	[HW_IMPRESORAS]	5			MA
	[HW_ESCANER]	5			MA
	[HW_SERVIDOR APLICACIONES]	5			MA
	[HW_SERVIDOR WEB]	5			MA
	[AUX_UPS SALA DE COMUNICACIONES]	5			A
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5			A
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5			A
[N.7] DESASTRES NATURALES. FENÓMENO SÍSMICO	[HW_COMPUTADORES DE ESCRITORIO]	5			M
	[HW_COMPUTADORES PORTÁTIL]	5			M
	[HW_IMPRESORAS]	5			M
	[HW_ESCANER]	5			M
	[HW_SERVIDOR APLICACIONES]	5			M
	[HW_SERVIDOR WEB]	5			M
	[AUX_UPS SALA DE COMUNICACIONES]	5			B
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5			M
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5			M

Fuente: William Salcedo Rodríguez

Tabla 18. Relacion de amenazas por origen desastres naturales

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO DIMENSIÓN %		
			[C]	[I]	[D]
[I.1] FUEGO	[HW_COMPUTADORES DE ESCRITORIO]	5			A
	[HW_COMPUTADORES PORTÁTIL]	5			A
	[HW_IMPRESORAS]	5			A
	[HW_ESCANER]	5			A
	[HW_SERVIDOR APLICACIONES]	5			MA
	[HW_SERVIDOR WEB]	5			MA
	[AUX_UPS SALA DE COMUNICACIONES]	5			MA
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5			MA
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5			MA
[I.2] DAÑOS POR AGUA	[HW_COMPUTADORES DE ESCRITORIO]	5			A
	[HW_COMPUTADORES PORTÁTIL]	5			A
	[HW_IMPRESORAS]	5			A
	[HW_ESCANER]	5			A
	[HW_SERVIDOR APLICACIONES]	5			MA
	[HW_SERVIDOR WEB]	5			MA
	[AUX_UPS SALA DE COMUNICACIONES]	5			MA
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5			MA
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5			MA
[I.3] CONTAMINACION MECÁNICA	[HW_COMPUTADORES DE ESCRITORIO]	10			M
	[HW_COMPUTADORES PORTÁTIL]	10			M
	[HW_IMPRESORAS]	10			M
	[HW_ESCANER]	10			M
	[HW_SERVIDOR APLICACIONES]	10			M
	[HW_SERVIDOR WEB]	10			M

Continuacion Tabla 18

	[AUX_UPS SALA DE COMUNICACIONES]	10	B
[I.4] CONTAMINACIÓN ELECTROMAGNÉTICA	[HW_COMPUTADORES DE ESCRITORIO]	10	MA
	[HW_COMPUTADORES PORTÁTIL]	10	MA
	[HW_IMPRESORAS]	10	A
	[HW_ESCANER]	10	A
	[HW_SERVIDOR APLICACIONES]	10	MA
	[HW_SERVIDOR WEB]	10	MA
	[AUX_UPS SALA DE COMUNICACIONES]	10	A
[I.5] AVERÍA DE ORIGEN FÍSICO O LÓGICO	[HW_COMPUTADORES DE ESCRITORIO]	50	A
	[HW_COMPUTADORES PORTÁTIL]	50	A
	[HW_IMPRESORAS]	50	A
	[HW_ESCANER]	50	A
	[HW_SERVIDOR APLICACIONES]	10	MA
	[HW_SERVIDOR WEB]	10	MA
	[AUX_UPS SALA DE COMUNICACIONES]	10	MA
	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	10	MA
	[SW_PLATAFORMA WEB]	10	MA
	[SW_SERVIDORES DE APLICACIONES]	10	MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	MA
[I.6] CORTE SUMINISTRO ELÉCTRICO	[HW_COMPUTADORES DE ESCRITORIO]	10	M
	[HW_COMPUTADORES PORTÁTIL]	10	M
	[HW_IMPRESORAS]	10	B
	[HW_ESCANER]	10	B
	[HW_SERVIDOR APLICACIONES]	10	MA
	[HW_SERVIDOR WEB]	10	MA
	[AUX_UPS SALA DE COMUNICACIONES]	10	B
[I.7] CONDICIONES INADECUADAS DE TEMPERATURA O HUMEDAD	[HW_COMPUTADORES DE ESCRITORIO]	10	M
	[HW_COMPUTADORES PORTÁTIL]	10	M
	[HW_IMPRESORAS]	10	B
	[HW_ESCANER]	10	B
	[HW_SERVIDOR APLICACIONES]	10	MA
	[HW_SERVIDOR WEB]	10	MA
	[AUX_UPS SALA DE COMUNICACIONES]	10	M

Continuacion Tabla 18

[I.8] FALLO DE SERVICIOS DE COMUNICACIONES	[COM_RED INALÁMBRICA]	70			A
	[COM_RED LOCAL]	50			MA
	[COM_INTERNET]	50			MA
[I.9] INTERRUPCIÓN DE OTROS SERVICIOS Y SUMINISTROS ESENCIALES	[AUX_UPS SALA DE COMUNICACIONES]	50			MA

Fuente: William Salcedo Rodríguez

Tabla 19. Relación de amenazas por errores y fallos no intencionados sobre activos

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %		
			[C]	[I]	[D]
[E.1] ERRORES DE LOS USUARIOS	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD ESTATAL]	10	MA	A	A
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	10	A	M	M
	[D_CONTRASEÑAS DE ACCESO DE EMPLEADOS]	5	M	M	B
	[S_CORREO ELECTRÓNICO INSTITUCIONAL]	70	A	M	M
	[S_SERVICIO DE ADMINISTRACIÓN SERVIDORES, MÁQUINAS VIRTUALES Y DISPOSITIVOS]	10	MA	M	M
	[S_SERVICIO DE DESARROLLO Y MANTENIMIENTO PLATAFORMAS DE LA ENTIDAD]	10	M	M	M
	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	10	A	M	A
	[SW_PLATAFORMA WEB]	10	A	M	A
	[SW_SERVIDORES DE APLICACIONES]	10	A	M	MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	A	M	A

Continuacion Tabla 19

[E.2] ERRORES DEL ADMINISTRADOR	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	10	MA	A	MA
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	10	M	M	MA
	[D_CONTRASEÑAS DE ACCESO DE EMPLEADOS]	5	M	M	M
	[S_CORREO ELECTRÓNICO INSTITUCIONAL]	10	A	M	A
	[S_SERVICIO DE ADMINISTRACIÓN SERVIDORES, MÁQUINAS VIRTUALES Y DISPOSITIVOS]	10	A	M	A
	[S_SERVICIO DE DESARROLLO Y MANTENIMIENTO PLATAFORMAS]	10	A	M	A
	[SW_PLATAFORMA WEB]	10	A	M	A
	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	10	A	M	A
	[SW_SERVIDORES DE APLICACIONES]	10	A	M	A
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	A	M	A
	[HW_COMPUTADORES DE ESCRITORIO]	50	M	B	M
	[HW_COMPUTADORES PORTÁTIL]	50	M	B	M
	[HW_SERVIDOR APLICACIONES]|	10	A	A	A
	[HW_SERVIDOR WEB]	10	A	MA	A
	[AUX_UPS SALA DE COMUNICACIONES]	10	A	M	A
	[COM_RED INALÁMBRICA]	10	M	M	B
	[COM_RED LOCAL]	10	A	M	A
	[COM_INTERNET]	10	M	M	A
	[AUX_UPS SALA DE COMUNICACIONES]	10	M	M	A
[E.8] DIFUSIÓN DE SOFTWARE DAÑINO	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	50	A	A	MA
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	10	A	A	MA
	[SW_PLATAFORMA WEB]	50	A	A	MA

Continuacion Tabla 19

	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	10	A	A	MA
	[SW_SERVIDORES DE APLICACIONES]	50	A	A	MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	50	A	A	MA
E.15] ALTERACIÓN ACCIDENTAL DE LA INFORMACIÓN	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	10	A	A	A
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	10	A	MA	MA
	[D_CONTRASEÑAS DE ACCESO DE EMPLEADOS]	10	M	A	M
	[SW_PLATAFORMA WEB]	10	MA	A	MA
	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	10	MA	A	A
	[SW_SERVIDORES DE APLICACIONES]	10	MA	A	MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	MA	MA	MA
[E.18] DESTRUCCIÓN DE INFORMACIÓN	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	5	MA	A	MA
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	5	MA	M	MA
	[SW_PLATAFORMA WEB]	5	MA	M	MA
	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	5	MA	A	A
	[SW_SERVIDORES DE APLICACIONES]	5	MA	M	A
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	A	MA	MA
[E.19] FUGAS DE INFORMACIÓN	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	5	MA	M	A
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	5	MA	M	A
	[SW_PLATAFORMA WEB]	5	MA	M	A
	[SW_SISTEMA DE BACKUPS EN EL SERVIDOR]	5	MA	A	A
	[SW_SERVIDORES DE APLICACIONES]	5	MA	A	A
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	MA	A	A
	[P_PERSONAL INTERNO]	50	A	A	M
[E.20] VULNERABILIDADES DE LOS PROGRAMAS (SOFTWARE)	[SW_SERVIDORES DE APLICACIONES]	10	MA	M	A
	[SW_PLATAFORMA WEB]	10	MA	M	A
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	50	MA	M	MA
	[SW_SERVIDOR DE FICHEROS]	10	MA	M	A
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	MA	M	MA

Continuacion Tabla 19

	[SW_OFIMÁTICA]	50	MA	M	M
	[SW_ANTIVIRUS]	50	A	M	M
	[SW_SISTEMA OPERATIVO]	50	M	M	A
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	5	A	M	A
	[SW_SISTEMA DE BACKUP]	5	M	M	M

Fuente: William Salcedo Rodríguez

Tabla 20. Relación de amenazas por ataques intencionados sobre activos

AMENAZA	ACTIVO	FRECUENCIA	IMPACTO PARA CADA DIMENSIÓN %		
			[C]	[I]	[D]
[A.5] SUPLANTACIÓN DE LA IDENTIDAD DEL USUARIO	[SW_SERVIDORES DE APLICACIONES]	5	MA	A	MA
	[SW_PLATAFORMA WEB]	5	MA	A	MA
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	5	MA	A	MA
	[SW_SERVIDOR DE FICHEROS]	5	MA	A	MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	MA	A	MA
	[SW_OFIMÁTICA]	10	A	M	A
	[SW_ANTIVIRUS]	10	A	M	A
	[SW_SISTEMA OPERATIVO]	10	A	A	A
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	5	A	A	MA
	[SW_SISTEMA DE BACKUP]	5	MA	MA	MA
[A.6] ABUSO DE PRIVILEGIOS DE ACCESO	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	10	MA	A	MA
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	10	MA	MA	A
	[SW_PLATAFORMA WEB]	10	A	MA	A
	[SW_SERVIDORES DE APLICACIONES]	10	A	MA	A
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	10	A	M	A
	[SW_SERVIDOR DE FICHEROS]	10	MA	M	A

Continuacion Tabla 20

	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	MA	A	MA
	[SW_OFIMÁTICA]	10	M	M	A
	[SW_ANTIVIRUS]	10	M	M	M
	[SW_SISTEMA OPERATIVO]	50	M	A	A
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	10	MA	A	MA
	[SW_SISTEMA DE BACKUP]	10	A	M	M
	[HW_COMPUTADORES DE ESCRITORIO]	50	M	M	M
	[HW_COMPUTADORES PORTÁTIL]	50	M	M	M
	[HW_IMPRESORAS]	50	B	B	M
	[HW_ESCANER]	50	B	B	M
	[HW_SERVIDOR APLICACIONES]|	10	A	A	MA
	[HW_SERVIDOR WEB]	10	A	A	MA
[A7] USO NO PREVISTO	[SW_SERVIDORES DE APLICACIONES]	10	A	M	MA
	[SW_PLATAFORMA WEB]	10	A	M	MA
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	10	M	A	MA
	[SW_SERVIDOR DE FICHEROS]	10	M	MA	MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	10	MA	M	MA
	[SW_OFIMÁTICA]	5	M	B	A
	[SW_ANTIVIRUS]	10	M	B	A
	[SW_SISTEMA OPERATIVO]	10	M	M	A
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	10	M	M	A
	[SW_SISTEMA DE BACKUP]	10	M	M	A
	[HW_COMPUTADORES DE ESCRITORIO]	10	M	A	M
	[HW_COMPUTADORES PORTÁTIL]	10	M	A	M
	[HW_IMPRESORAS]	10	M	M	B

Continuacion Tabla 20

	[HW_ESCANER]	10	B	B	B
	[HW_SERVIDOR APLICACIONES]|	10	M	M	MA
	[HW_SERVIDOR WEB]	10	M	M	MA
	[AUX_UPS SALA DE COMUNICACIONES]	10	A	M	A
	[COM_RED INALÁMBRICA]	10	M	A	MA
	[COM_RED LOCAL]	10	M	M	A
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5	M	M	MA
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5	M	A	MA
[A.8] DIFUSIÓN DE SOFTWARE DAÑINO	[SW_SERVIDORES DE APLICACIONES]	5	A	M	A
	[SW_PLATAFORMA WEB]	5	A	M	A
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	5	M	M	A
	[SW_SERVIDOR DE FICHEROS]	5	A	M	A
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	M	A	A
	[SW_OFIMÁTICA]	50	A	M	M
	[SW_ANTIVIRUS]	50	M	M	A
	[SW_SISTEMA OPERATIVO]	50	M	A	A
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	10	A	M	A
	[SW_SISTEMA DE BACKUP]	5	A	M	A
[A.11] ACCESO NO AUTORIZADO	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	5	A	A	MA
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	5	A	A	MA
	[SW_PLATAFORMA WEB]	5	A	A	MA
	[SW_SERVIDORES DE APLICACIONES]	5	A	A	MA
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	10	A	M	A
	[SW_SERVIDOR DE FICHEROS]	10	MA	A	A
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	A	A	MA
	[SW_OFIMÁTICA]	50	A	MA	MA
	[SW_ANTIVIRUS]	5	M	M	A
	[SW_SISTEMA OPERATIVO]	50	A	M	A
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	5	A	MA	A
	[SW_SISTEMA DE BACKUP]	5	MA	A	A

Continuacion Tabla 20

	[HW_COMPUTADORES DE ESCRITORIO]	50	M	M	M
	[HW_COMPUTADORES PORTÁTIL]	50	M	M	M
	[HW_IMPRESORAS]	70	B	B	M
	[HW_ESCANER]	50	B	B	B
	[HW_SERVIDOR APLICACIONES]|	5	A	A	MA
	[HW_SERVIDOR WEB]	5	MA	A	MA
	[AUX_UPS SALA DE COMUNICACIONES]	5	B	B	A
	[COM_RED INALÁMBRICA]	50	M	M	A
	[COM_RED LOCAL]	10	A	M	MA
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5	A	A	MA
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5	A	A	MA
[A.13] REPUDIO	[S_CORREO ELECTRÓNICO INSTITUCIONAL]	10		M	M
	[S_SERVICIO DE ADMINISTRACIÓN SERVIDORES, MÁQUINAS VIRTUALES Y DISPOSITIVOS]	10		M	M
	[S_SERVICIO DE DESARROLLO Y MANTENIMIENTO PLATAFORMAS]	10		M	M
[A.14] INTERCEPTACIÓN DE INFORMACIÓN	[SW_SERVIDORES DE APLICACIONES]	5	A	A	
	[SW_PLATAFORMA WEB]	5	A	A	
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	10	A	MA	
	[SW_SERVIDOR DE FICHEROS]	10	A	MA	
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	A	M	
	[COM_RED INALÁMBRICA]	50	A	A	
	[COM_RED LOCAL]	50	A	A	
[A.15] MODIFICACIÓN DELIBERADA DE LA INFORMACIÓN	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	5		MA	
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	5		A	
	[SW_PLATAFORMA WEB]	5		MA	
	[SW_SERVIDORES DE APLICACIONES]	5		MA	
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	5		MA	
	[SW_SERVIDOR DE FICHEROS]	5		MA	
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5		MA	
	[SW_OFIMÁTICA]	50		A	
	[SW_ANTIVIRUS]	50		A	
	[SW_SISTEMA OPERATIVO]	50		A	

Continuacion Tabla 20

	[SW_GESTOR DE MÁQUINAS VIRTUALES]	5	MA	
	[SW_SISTEMA DE BACKUP]	5	MA	
[A.18] DESTRUCCIÓN DE LA INFORMACIÓN	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	5	A	MA
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	5		MA
	[SW_PLATAFORMA WEB]	5		MA
	[SW_SERVIDORES DE APLICACIONES]	5		MA
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	5		MA
	[SW_SERVIDOR DE FICHEROS]	5		MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5		MA
	[SW_OFIMÁTICA]	50		A
	[SW_ANTIVIRUS]	50		A
	[SW_SISTEMA OPERATIVO]	50		M
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	5		MA
	[SW_SISTEMA DE BACKUP]	5		MA
[A.19] REVELACIÓN DE INFORMACIÓN	[D_CÓDIGO FUENTE DEL PORTAL WEB DE LA ENTIDAD]	5		
	[D_ARCHIVO DE COPIAS DE SEGURIDAD DE LA INFORMACIÓN]	5	MA	
	[SW_PLATAFORMA WEB]	5	MA	
	[SW_SERVIDORES DE APLICACIONES]	5	MA	
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	10	MA	
	[SW_SERVIDOR DE FICHEROS]	10	MA	
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5	MA	
	[SW_GESTOR DE MÁQUINAS VIRTUALES]	5	MA	
	[SW_SISTEMA DE BACKUP]	5	MA	
[A.23] MANIPULACIÓN DE LOS EQUIPOS	[HW_COMPUTADORES DE ESCRITORIO]	10	M	A
	[HW_COMPUTADORES PORTÁTIL]	10	M	A
	[HW_IMPRESORAS]	50	B	M
	[HW_ESCANER]	50	B	M
	[HW_SERVIDOR APLICACIONES]	5	MA	MA
	[HW_SERVIDOR WEB]	5	MA	MA
	[AUX_UPS SALA DE COMUNICACIONES]	5	A	MA
[A.24] DENEGACIÓN DE SERVICIOS	[S_CORREO ELECTRÓNICO INSTITUCIONAL]	5		MA

Continuacion Tabla 20

	[S_SERVICIO DE ADMINISTRACIÓN SERVIDORES, MÁQUINAS VIRTUALES Y DISPOSITIVOS]	5			MA
	[S_SERVICIO DE DESARROLLO Y MANTENIMIENTO PLATAFORMAS]	5			MA
	[SW_PLATAFORMA WEB]	5			MA
	[SW_SERVIDORES DE APLICACIONES]	5			MA
	[SW_SERVIDOR DE CORREO ELECTRÓNICO]	5			MA
	[SW_SERVIDOR DE FICHEROS]	5			MA
	[SW_SISTEMA DE GESTIÓN DE BASES DE DATOS]	5			MA
[A.25] ROBO	[HW_COMPUTADORES DE ESCRITORIO]	5			A
	[HW_COMPUTADORES PORTÁTIL]	5			A
	[HW_IMPRESORAS]	5			A
	[HW_ESCANER]	5			M
	[HW_SERVIDOR APLICACIONES]|	5			MA
	[HW_SERVIDOR WEB]	5			MA
	AUX_UPS SALA DE COMUNICACIONES]	5			MA
[A.26] ATAQUE DESTRUCTIVO	[HW_COMPUTADORES DE ESCRITORIO]	5			A
	[HW_COMPUTADORES PORTÁTIL]	5			A
	[HW_IMPRESORAS]	5			A
	[HW_ESCANER]	5			M
	[HW_SERVIDOR APLICACIONES]|	5			MA
	[HW_SERVIDOR WEB]	5			MA
	AUX_UPS SALA DE COMUNICACIONES]	5			MA
	[L_OFICINA DE GESTION INFORMATICA PRINCIPAL]	5			MA
	[L_OFICINA DE GESTION INFORMATICA SECUNDARIA]	5			MA
[A.28] INDISPONIBILIDAD DEL PERSONAL	[P_PERSONAL INTERNO]	10			A
[A.29] EXTORSIÓN	[P_PERSONAL INTERNO]	5	A	A	A
[A.30] INGENIERÍA SOCIAL	[P_PERSONAL INTERNO]	10	MA	A	A

Fuente: William Salcedo Rodríguez

10.3 FASE 3. DISEÑO DE CONTROLES DE SEGURIDAD

Una vez realizado el inventario de activos, e identificadas las amenazas y vulnerabilidades, el siguiente paso es diseñar los controles que permitirán reducir el riesgo.

Las salvaguardas están definidas por la norma ISO 27001, según la amenaza identificada, el tipo de tratamiento a implementar está definido por el método de gestión de riesgos MAGERIT, las cuales se describen a continuación:

Tipos de salvaguardas:

- [PR] Preventivas
- [DR] disuasorias
- [EL] eliminatorias
- [IM] minimizadoras
- [CR] correctivas
- [RC] recuperativas
- [MN] de monitorización
- [DC] de detección
- [AW] de concienciación
- [AD] administrativas

Los controles a implementar se centrarán sobre las principales amenazas en los activos de la entidad estatal, a continuación, se describe el listado de salvaguardas sobre los activos:

SW_PLATAFORMA WEB

[HW_SERVIDOR WEB

Tabla 21. Listado de salvaguardas sobre los principales activos

ACTIVO	AMENAZA	TIPO	CONTROLES ISO 27001	SALVAGUARDAS
[SW_PLATAFORMA WEB]	[E2] Errores del administrador	[DC] Detección [DR] disuasorias [AD] administrativas	7.2.2, 12.4.3, 12.6.1, 14.1.1, 14.1.2, 14.2.1, 14.2.5, 14.2.8, 14.2.9, 14.3.1	✓ Concientizar al personal interno y los contratistas externos sobre las políticas y procedimientos de seguridad. ✓ Registrar todas las actividades del administrador del sistema de informacion, las bitácoras se deben de resguardar y revisar periódicamente. ✓ Identificar las principales vulnerabilidades técnicas de los sistemas de información usados; evaluar la exposición de la entidad estatal a estas vulnerabilidades, y tomar las políticas de control que permitan minimizar los riesgos. ✓ Los requisitos relacionados con la entidad de la información se deberían incluir en los requisitos para nuevos SI o para mejoras en los sistemas de información existentes. ✓ Proteger de actividades fraudulentas, la información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas. ✓ Establecer reglas y políticas de seguridad al desarrollo de software propio en la entidad estatal. ✓ Establecer, documentar y mantener principios para la construcción de sistemas seguros. ✓ Hacer seguimiento a la actividad de desarrollo de sistemas contratados externamente.

Continuacion Tabla 21

				✓ Establecer programas de pruebas para aceptación y criterios de aceptación relacionados, para sistemas de información nuevos, actualizaciones y nuevas versiones.
[SW_PLATAFORMA WEB]	[E8] Difusión de software dañino	[DC] Detección [IM] minimizadoras	7.1.2, 12.2.1, 12.6.2	✓ Establecer las responsabilidades de la seguridad de la información sobre los acuerdos contractuales con personal interno y externo. ✓ Implementar controles de detección, prevención, recuperación y conciencia apropiada de los usuarios para proteger la informacion contra códigos maliciosos. ✓ Establecer e implementar reglas para la instalación de software por parte de los usuarios.
[SW_PLATAFORMA WEB]	[E19] Fugas de informaci ón	[DC] Detección [DR] disuasorias [IM] minimizadoras	7.2.2, 9.4.1, 9.4.2, 9.4.3, 8.2.1, 12.3.1, 14.2.8, 14.3.1, 16.1.1, 16.1.2, 16.1.4, 16.1.5, 16.1.6, 16.1.7	✓ Concientizar al personal interno y los contratistas externos sobre las políticas y procedimientos de seguridad. ✓ Restringir el acceso a la información y a las funciones de los sistemas de las aplicaciones, de acuerdo con la política de control de acceso. ✓ Controlar el acceso a sistemas y aplicaciones mediante un proceso de ingreso seguro ✓ Establecer una política de creación de contraseñas robustas, con periodo de caducidad.

Continuacion Tabla 21

				✓ Clasificar la información en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. ✓ Realizar copias de respaldo de la Información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con las políticas de copias de respaldo. ✓ Realizar pruebas de funcionalidad de la seguridad, durante el desarrollo del software. ✓ Seleccionar, proteger y controlar cuidadosamente, la informacion producto de pruebas sobre el software.
[SW_PLATAFORMA WEB]	[E19] Fugas de informaci ón	[DC] Detección [AW] de concienciac ión	7.2.2, 9.4.1, 9.4.2, 9.4.3, 8.2.1, 12.3.1, 14.2.8, 14.3.1, 16.1.1, 16.1.2, 16.1.4, 16.1.5, 16.1.6, 16.1.7	Capacitar el personal interno y los contratistas externos sobre las políticas y procedimientos de seguridad de la informacion. Identificar cuales eventos de seguridad de la información deben de ser clasificados como incidentes de seguridad de la información. Responder a los incidentes de seguridad de la información de acuerdo a procedimientos documentados. Apropiar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la Información, para reducir la posibilidad o el impacto de incidentes futuros.

Continuacion Tabla 21				Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que sirva como evidencia.
[SW_PLATAFORMA WEB]	[E20] Vulnerabilidades de los programas	[DC] Detección	18.1.5, 10.1.1, 10.1.2	Diseñar controles criptográficos en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. Diseñar e implementar políticas sobre el uso de controles criptográficos para la protección de la información. Diseñar e implementar políticas sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
[SW_PLATAFORMA WEB]	[E20] Vulnerabilidades de los programas	[DC] Detección [PR] Preventivas	18.1.5, 10.1.1, 10.1.2, 14.2.1, 14.2.5, 14.2.8, 14.2.9.	Establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de SI. Realizar pruebas de funcionalidad de la seguridad, durante el desarrollo del software. Establecer programas de pruebas para aceptación y criterios de aceptación relacionados, para sistemas de información nuevos, actualizaciones y nuevas versiones. Seleccionar, proteger y controlar cuidadosamente, la informacion producto de pruebas sobre el software.

Continuacion Tabla 21

[SW_PLATAFORMA WEB]	[E21] Errores de mantenimiento/ actualización software	[DC] Detección [PR] Preventivas	12.1.1, 12.2.1, 12.6.2, 14.2.2, 14.2.5,	Implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos. Establecer e implementar las reglas para la instalación de software por parte de los usuarios.
[SW_PLATAFORMA WEB]	[A5] Suplantación de la Identidad del Usuario	[DC] Detección	7.2.3, 9.1.1, 9.2.1, 9.2.2, 9.2.3, 9.4.3,	Establecer procedimientos para emprender acciones en contra de los empleados, deben de ser debidamente documentadas y socializadas con el personal interno. Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. Implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.

Continuacion Tabla 21

[SW_PLATAFORMA WEB]	[A5] Suplantación de la Identidad del Usuario	[DC] Detección	7.2.3, 9.1.1, 9.2.1,	Restringir y controlar la asignación y uso de derechos de acceso privilegiado. Establecer políticas de creación de contraseñas robustas.
[SW_PLATAFORMA WEB]	[A8] Difusión de software dañino	[DC] Detección	12.2.1, 14.2.2.	Implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios para proteger contra códigos maliciosos. Controlar los cambios a los sistemas dentro del ciclo de vida del desarrollo mediante el uso de procedimientos formales de control de cambios.
[SW_PLATAFORMA WEB]	[A15] Modificación deliberada de la información	[DC] Detección	12.3.1, 14.1.1, 16.1.5	Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Incluir los requisitos relacionados con seguridad de la información en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

Continuacion Tabla 21

[SW_PLATAFORMA WEB]	[A18] Destrucción de informaci ón	[DC] Detección	12.3.1, 14.1.1, 16.1.5	Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Incluir los requisitos relacionados con seguridad de la información en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes. Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
[HW_SERVIDOR WEB]	[N1] Fuego	[DC] Detección	11.1.4	Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.
[HW_SERVIDOR WEB]	[N8]Desa stres Naturales Fenómen o de Origen Volcánico	[DC] Detección	11.1.4	Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.
[HW_SERVIDOR WEB]	[I1] Fuego	[DC] Detección	11.1.4	Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes.

Continuacion Tabla 21

[HW_SERVIDOR WEB]	[I*] Desastres Industriales	[DC] Detección	11.1.1, 11.1.3, 11.2.2, 11.2.3	Definir perímetros de seguridad en instalaciones de manejo de información. Diseñar y aplicar seguridad física a oficinas, Proteger contra falla de energía y Otras interrupciones causadas por fallas en los servicios de suministros. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información debe de estar protegido contra interceptación, interferencia o daño.
[HW_SERVIDOR WEB]	[I3] Contaminación Mecánica	[[DC] Detección	11.2.1	Adecuar la sala de sistemas informáticos con las medidas de protección física, que eviten la contaminación física de los equipos y servidores.
[HW_SERVIDOR WEB]	[I4] Contaminación Electromagnética	[DC] Detección	11.2.2, 11.2.3	Proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debería proteger contra interceptación, interferencia o daño.
[HW_SERVIDOR WEB]	[I5] Avería de Origen Físico o lógico	[DC] Detección	11.2.1, 11.2.4	Adecuar la sala de sistemas informáticos con las medidas de protección física, que eviten la contaminación física de los equipos y servidores.

Continuacion Tabla 21

[HW_SERVIDOR WEB]	[I6] Corte del suministro eléctrico	[DC] Detección	11.2.2, 11.2.3	Proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros. El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debería proteger contra interceptación, interferencia o daño.
[HW_SERVIDOR WEB]	[I7] Condiciones inadecuadas de temperatura o humedad	[DC] Detección	11.1.4, 11.2.1	Diseñar y aplicar protección física contra desastres naturales, ataques maliciosos y accidentes. Adecuar la sala de sistemas informáticos con las medidas de protección física, que eviten la contaminación física de los equipos y servidores.
[HW_SERVIDOR WEB]	[E2] Errores del administrador	[DC] Detección	7.2.1, 17.2.1	Exigir a todos los empleados y contratistas la aplicación de la seguridad de la información. Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

Continuacion Tabla 21

[HW_SERVIDOR WEB]	[E23] Errores de mantenimiento/actualización de equipos	[DC] Detección	11.2.4, 12.1.2, 17.2.1,	Crear planes de mantenimiento preventivos sobre servidores y equipos para asegurar su disponibilidad. Crear bitácoras que permitan controlar los cambios en la entidad estatal, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información. Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
[HW_SERVIDOR WEB]	[E25] Pérdida de equipos/robo	[DC] Detección	11.1.1, 11.1.2, 11.1.3, 11.2.1	Definir perímetros de seguridad, para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. Proteger las áreas críticas mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. Implementar controles de seguridad física a oficinas, recintos e instalaciones.

Continuacion Tabla 21				Proteger el acceso a equipos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.
[HW_SERVIDOR WEB]	[A6] Abuso de privilegios de acceso	[DC] Detección	11.1.2, 11.1.3	Proteger el acceso a equipos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado. Implementar controles de seguridad física a oficinas, recintos e instalaciones.
[HW_SERVIDOR WEB]	[A11] Acceso no autorizado	[DC] Detección	11.1.2, 11.1.3	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. Diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
[HW_SERVIDOR WEB]	[A23] Manipulación de los equipos	[DC] Detección	11.1.2, 11.1.3	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones. Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.

Continuacion Tabla 21

[HW_SERVIDOR WEB]	[A24] Denegación de servicio	[DC] Detección	17.1.1, 17.1.2, 17.1.3	Establecer los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas. Establecer y mantener procesos y controles para asegurar el nivel de continuidad requerido, para la seguridad de la información durante una situación adversa. Implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
[HW_SERVIDOR WEB]	[A25] Robo	[DC] Detección	11.1.1, 11.1.2, 11.1.3, 11.2.1	Establecer perímetros de seguridad para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información. Proteger las áreas críticas mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado. Proteger el acceso a equipos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

Fuente: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

11 POLITICAS DE SEGURIDAD NORMA ISO 27001

Las politicas son mecanismos, procedimientos, controles que ayudan a mitigar las vulnerabilidades a los que están expuestos los activos.

Cada una de las politicas que se especifican a continuación contiene una serie de instrucciones aplicadas dependiendo las valoraciones o impactos sobre las amenazas que sufren los activos.

Tabla 22. Politicas de seguridad propuestas según Norma ISO 27001

Declaración de Aplicabilidad			
REF	**Punto de Control ISO 27001**	**Aplica**	**Como se Aplica el Control**
A.5	**Políticas de seguridad de la información**		
A.5.1	**Gestión de la Gerencia para la seguridad de la información**		
A.5.1.1	Políticas de la seguridad de de la información	SI	• Definir el conjunto de politicas paea la seguridad de la informacion. • Dar a conocer las politicas de informacion al personal interno de la organización.
A.5.1.2	Revisión de las políticas de seguridad de la información	No	
A.6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A.6.1.1	Funciones y responsabilidades de la seguridad de la información	Si	• El administrador del sistema de informacion es el principal responsable de la seguridad de la informacion. • El administrado del sistema puede delegar funciones a su equipo colaborador pero bajo su supervision.
A.6.1.2	Segregación de tareas	NO	
A.6.1.3	Contacto con las autoridades	NO	
A.6.1.4	Contacto con las autoridades	NO	
A.6.1.5	Seguridad de la información en la gestión del proyecto	NO	
A.6.2	**Equipos móviles y trabajo a distancia**		
A.6.2.1	Política de los equipos móviles	Si	• Proteger los dispositivos moviles (Celular, Tablets) con aplicación antivirus. • Debe existir una red wifi de visitantes para evitar que se conecten a la red interna y puedan tener acceso a informacion privada.
A.6.1.8	Trabajo a distancia	NO	

Continuacion Tabla 22			
A.7	**Seguridad de los recursos humanos**		
A.7.1	**Antes de reclutarlo**		
A.7.1.1	Filtración	Si	
A.7.1.2	Términos y condiciones del empleo	Si	
A.7.2	**Durante el trabajo**		
A.7.2.1	Responsabilidades de la Gerencia	NO	
A.7.2.2	Concientización, educación y capacitación sobre seguridad de la información	Si	• Los usuarios que tienen acceso a informacion confidencial o critica, deben de estar capacitados sobre las politicas de seguridad de la informacion para su adecuado manejo. • Se debe concientizar a los usuarios sobre las politicas de seguridad basicas para resguardar la seguridad de la informacion, por ejemplo: Evitar abrir archivos adjntos de remitentes de correo electronico desconocidos, evitar hacer uso de medios extraibles como pendrive que puedan contener software malicioso.
A.7.2.3	Procesos disciplinarios	Si	• Definir sanciones o procesos disciplinarios en caso de que se evidencia manejo erroneo de la informacion la cual la ponga en riesgo por parte de los usuarios de la organización.
A.7.3	**Término y cambio de empleo**		
A.7.3.1	Término o cambio de responsabilidades de empleo	NO	
A.8	**Gestión de los Activos**		
A.8.1	**Responsabilidades sobre los activos**		
A.8.1.1	Inventario de activos	Si	• Los activos de la entidad deben estar identificados y clasificados, facilitando su control y seguridad.
A.8.1.2	Propiedad de los activos	Si	• Limitar el acceso a los activos y recursos informaticos para evitar que usuarios no autorizados tengan acceso a estos. • Definir responsables sobre activos, por ejemplo los activos como servidores son responsabilidad del administrador del sistema y nadie mas puede tener acceso.
A.8.1.3	Uso aceptable de los activos	NO	

Continuacion Tabla 22			
A 8.1.4	Retorno de los Activos	Si	• Documentar la asignacion de equipos informaticos a los usuarios por medio de actas en la cuales se aclara la responsabilidad del uso adecuado de los equipos y la informacion de la organización interna y externamente.
A.8.2	**Clasificación de la información**		
A.8.2.1	Clasificación de la información	Si	• Los datos criticos como bases de datos y sistemas de informacion se deben clasificar y asignar responsables de su manejo, con el fin de evitar uso inadecuado de personal no autorizado.
A.8.2.2	Etiquetado de la información	NO	
A 8.2.3	Manejo de los activos	NO	
A.8.3	**Manejo de los medios de comunicación**		
A.8.3.1	Gestión de medios de comunicación removibles	Si	• Deshabilitar el acceso a medios de almacenamiento externo en equipos no autorizados. • Tener un sistema de antivirus robusto en los equipos y administrado desde una consola central con el fin de identificar amenazas originadas desde medios de almacenamiento externo.
A.8.3.2	Disposición de los medios comunicación	NO	
A.8.3.3	Transferencias física de los medios de comunicación	Si	• Los medios de almacenamiento externo como discos externos, DVD, Unidades usb, que contengan informacion critica deben estar a cargo de un responsable encargado de salvaguardarlo. Se puede cifrar la informacion contenida en estos medios para evitar que personal no autorizado tenga acceso a estos datos.
A.9	**Control de acceso**		
A.9.1	**Requisitos del negocio sobre control del acceso**		
A.9.1.1	Política de control de acceso	Si	• Establecer politicas de acceso al Datacenter, bases de datos y aplicativos, de tal manera que solo el personal autorizado los pueda accesar. • Documentar estas politicas de acceso y asignar roles y funciones dentro de la organizacion que facilitan la administracion de los permisos a la informacion.
A.9.1.2	Acceso a la redes y a los servicios de las redes	NO	

Continuacion Tabla 22

A.9.2	**Gestión del acceso al usuario**		
A.9.2.1	Registro y des-registro del usuario	Si	• Al ingresar un usuario nuevo a la compañía se debe diligenciar un formato en la cual se establece su perfil interno, tipo de informacion o acceso que necesita, permisos de navegacion. • El area de gestion Humana debe de informar al departamento de sistemas sobre la creacion de un nuevo usuario y la desvinculacion de usuarios dentro de la compañia, con el fin de actualizar los permisos de acceso a la informacion por parte de los usuarios.
A.9.2.2	Provisión de acceso al usuario	NO	
A.9.2.3	Gestión de los derechos de acceso privilegiado	Si	• Controlar el acceso a la informacion por parte de los usuarios a traves del directorio activo, estableciendo perfiles y roles que facilitan la administracion de los recursos informaticos a los cuales los usuarios tienen acceso.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	NO	
A.9.2.5	Verificación de los derechos de acceso de los usuarios	NO	
A.9.2.6	Retiro o ajuste de los derechos de acceso	Si	• El area de gestion humana debe informar oportunamente sobre las novedades de personal, desvinculacion de usuarios y cambios de perfiles y ascensos en la compañía con el fin de facilitar al administrador del sistema el control de acceso y perfiles de los usuarios, de esta forma evitar accesos no autorizados y vulnerabilidades de seguridad sobre el sistema de informacion.
A.9.3	**Responsabilidades del usuario**		
A.9.3.1	Uso de información secreta de autenticación	NO	
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción del acceso a la información	Si	• Implementar servidor de dominio con un directorio activo que facilite el control de permisos a los usuarios por medio de perfiles. • Contar con un Firewall que filtre la entrada y salida de informacion por medio de politicas según los perfiles establecidos en el servidor de dominio.

Continuacion Tabla 22

A.9.4.2	Procedimiento seguro de logeo	Si	• Cada usuario en la organización que requiera acceso al sistema de informacion o aplicativos de la compañía debe de tener un usuario de dominio creado con su respectivo perfil, garantizando la autenticacion del mismo y facilitando la administracion de los controles de acceso a la informacion por parte de los usuarios.
A.9.4.3	Sistema de gestión de la clave	Si	• Establecer contraseñas de acceso robustas que eviten el acceso a los equipos informaticos por personal no autorizado. • Las contraseñas deben de tener una caducidad y facilitar al usuario su cambio. • Las contraseñas de acceso deben ser intrasferibles y se debe informar a los usuarios las sanciones disciplinarias por transferir datos de acceso a personal no autorizado.
A.9.4.4	Uso de programas utilitarios de privilegio	Si	• Establecer tipos de usuario en los equipos informaticos, dando permisos de administrador solo a personal autorizado para realizar cambios sobre el sistema opertaivo. • Bloquear el acceso a medios de almacenamiento extraible y unidades opticas en equipos no autorizados. • Contar con sistema de antivirus robusto y administrado por consola central que permita identificar cambios sobre el sistema operativo en los equipos informaticos.
A.9.4.5	Control del acceso para programar el código fuente	Si	• El codigo fuente de las aplicaciones principales de la organizacion debe estar restringido, el administrador del sistema de informacion es responsable de este activo.
A.10		**Criptografía**	
A.10.1		**Controles de la criptografía**	
A.10.1.1	Política del uso de controles criptográficos	Si	• Crear politicas para la encriptacion de informacion critica como Backups de bases de datos o Backups de informacion critica de usuarios en la organización.
A.11		**Seguridad física y medioambiental**	
A.11.1		**Áreas seguras**	
A.11.1.1	Perímetro de seguridad física	Si	• Los servidores de bases de datos, los equipos de comunicación, rack de comunicaciones, copias de seguridad en medios externos como discos duros, DVD, deben estar ubicados en datacenter con control fisico de acceso de tipo biométrico.

Continuacion Tabla 22			
A.11.1.2	Controles físicos de los ingresos	NO	
A.11.1.3	Seguridad de las oficinas, salas e instalaciones	NO	
A.11.1.4.	Protección contra las amenazas externas y medioambientales	Si	• El datacenter en el cual estan alojados los servidores y equipos de telecomunicaciones, debe estar adecuado con un sistema de respaldo UPS que garantice la disponibilidad de la informacion en caso de presentarse corte de fluido electrico, • Debe contar con un sistema de refrigeracion que evite el sobrecalentamiento de los equipos. • Debe contar con un tablero electrico dedicado y sistema de polo a tierra que proteja los equipos de fallas o cortos eléctricos. • Debe contar con sistema de deteccion de humo y extintores debidamente señalizados ante algun incendio o corto electrico en los equipos.
A.11.1.5	Trabajo en áreas seguras	NO	
A.11.1.6	Distribución de las zonas de carga	NO	
A.11.2			**Equipos**
A.11.2.1	Ubicación y protección de los equipos	NO	
A.11.2.2	Servicios públicos de soporte	Si	• Debe existir un sistema de proteccion UPS dedicado para el datacentecenter, tambien se puede implementar una planta electrica externa que de un respaldo a las UPS del datacenter en caso de cortes electricos muy extensos. • Los equipos informaticos que no pertenecen al datacenter deben estar protegidos por un sistema de respaldo UPS independiente y dedicado a estos equipos.
A.11.2.3	Seguridad en el cableado	Si	• El datacenter debe de contar con Rack de comunicaciones con un cableado estructurado debidamente ordenado y etiquetado. • Cada puesto de trabajo debe contar con su punto de datos y voz debidamente etiquetado.

Continuacion Tabla 22			
A.11.2.3	Seguridad en el cableado	Si	• Debe existir un circuito electrico de red regulada la cual esta conectada con el sistema de respaldo UPS, un sistema de red electrica no regulada en la cual no necesitamos proteccion de la UPS. • Se deben realizar inspecciones continuas sobre el estado fisico del cableado electrico y de datos en el datacenter y areas de trabajo en la compañia con el fin de identificar deterioro o falla y poder tomar las correciones con el debido tiempo.
A.11.2.4	Mantenimiento de los equipos	Si	• Se debe crear un plan de mantenimiento preventivo sobre los equipos informaticos con el fin de identificar fallas que puedan causar el mal funcionamiento de los equipos y garantizando la disponibilidad de la informacion alli almacenada.
A.11.2.5	Retiro de los activos	Si	• Se debe de crear acta de confidencialidad por cada usuario en el cual se aclara su responsabilidad sobre el uso del equipo a cargo y la informacion de la organizacion. • Los responsables de activos de informacion o equipos informaticos son responsables de su traslado o uso externo, el cual debe estar previamente autorizado por el deparatmento de sistemas.
A.11.2.6	Seguridad de los equipos y bienes fuera de las instalaciones	NO	
A.11.2.7	Disposición o re-uso seguro de los equipos	NO	
A.11.2.8	Usuario de equipo abandonado	NO	
A.11.2.9	Política de escritorio y pantallas limpias	NO	
A.12	**Seguridad de las operaciones**		
A.12.1	**Procedimientos y responsabilidades operaciones**		
A.12.1.1	Documentación de los procedimientos operacionales	NO	
A.12.1.2	Cambios en la gerencia	NO	
A.12.1.3	Gestión de la capacidad	NO	
A.12.1.4	Separación de ambientes de desarrollo, prueba y de operaciones	NO	

Continuacion Tabla 22			
A.12.2	**Protección contra el malware (programa malicioso)**		
A.12.2.1	Controles contra el malware	Si	• Contar con sistema de antivirus robusto y administrado por consola central que permita identificar cambios sobre el sistema operativo en los equipos informaticos.
A.12.3	**Backup**		
A.12.3.1	Backup de la información	Si	• Crear politicas de copias de seguridad sobre las principales bases de datos de la organización, las copias deben realizarse en un horario que no afecte los procesos diarios de la organización, se pueden almacenar en un servidor externo o en un medio extraíble. • Se debe llevar control por escrito del proceso estableciendo responsables de la creacion del backup y responsable del resguardo del mismo.
A.12.4	**Logeo y monitoreo**		
A.12.4.1	Eventos de logeo	NO	
A.12.4.2	Protección de la información del logeo	NO	
A.12.4.3	Logeo del administrador y operador	NO	
A.12.4.4	Sincronización de los relojes	NO	
A.12.5	**Control del software operacional**		
A.12.5.1	Instalación del software en los sistemas operacionales	Si	• Establecer los tipos de usuario en los equipos informaticos, dando permisos de administrador solo a el personal autorizado de realizar cambios sobre el sistema operativo. • Bloquear el acceso a medios de almacenamiento extraible y unidades opticas en equipos no autorizados. • Contar con sistema de antivirus robusto y administrado por consola central que permita identificar cambios sobre el sistema operativo en los equipos informaticos.
A.12.6	**Gestión de las vulnerabilidades técnicas**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	NO	
A.12.6.2	Restricciones en la instalación de software	NO	

Continuacion Tabla 22			
A.12.7	**Consideraciones de las auditorías sobre los sistemas de información**		
A.12.7.1	Controles de la auditoría sobre los sistemas de información	NO	
A.13	**Seguridad de las comunicaciones**		
A.13.1	**Gestión de la seguridad de las redes**		
A.13.1.1	Controles en las redes	NO	
A.13.1.2	Seguridad de los servicios de las redes	NO	
A.13.1.3	Segregación en las redes	Si	• Los servidores de aplicativos y bases de datos deben pertenecer a un segmento de red diferente dentro de la organización por medio de una VLAN, de esta manera evitar que sean facilmente visualizados por los equipos informaticos de la compañía que hacen parte de otro segmento, esto con el fin de reducir la posibilidad de ataques informaticos internos. • Debe existir una red wifi que hace parte de la intranet para uso exclusivo de equipos informaticos autorizados y una red wifi que no hace parte de la intranet para visitantes y usuarios que no requieren acceso a los aplicativos o bases de datos internos.
A.13.2	**Transferencia de la información**		
A.13.2.1	Políticas y procedimientos de la transferencia de la información	No	
A.13.2.2	Acuerdos sobre la transferencias de la información	No	
A.13.2.3	Mensajes electrónicos	Si	• Contar con sistema de antivirus robusto con modulo antispam y administrado por consola central que permita identificar cambios sobre el sistema operativo en los equipos informaticos.
A.13.2.4	Confidencialidad o acuerdos no divulgados	No	
A.14	**Adqusición, desarrollo y mantenimiento del sistema**		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
A.14.1.1	Análisis y especificaciones de los requisitos de la seguridad de la información	Si	• Las politicas de seguridad sobre los activos de informacion deben estar debidamente documentadas y ser aplicadas tanto a los sistemas informaticos y de informacion existentes como tambien al nuevo software o sistema informatico que se desee implementar.

Continuacion Tabla 22			
A.14.1.2	Seguridad de los servicios de aplicación en las redes públicas	NO	
A.14.1.3	Protección de las transacciones de los servicios de aplicación	No	
A.14.2	**Seguridad en los procesos del programa de desarrollo y soporte**		
A.14.2.1	Política del programa de desarrollo seguro	NO	
A.14.2.2	Procedimiento de control de los cambios de sistemas	NO	
A.14.2.3	Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional	NO	
A.14.2.4	Restricciones a los cambios de los paquetes de software	NO	
A.14.2.5	Principios del sistema de seguridad para la ingeniería	NO	
A.14.2.6	Ambiente seguro del programa de desarrollo	NO	
A.14.2.7	Programa de desarrollo subcontratado	NO	
A.14.2.8	Revisión de la seguridad del sistema	NO	
A.14.2.9	Revisión de la aceptación del sistema	NO	
A.14.3	**Datos de prueba**		
A.14.3.1	Protección de los datos de prueba	NO	
A.15	**Relación con los proveedores**		
A.15.1	**Seguridad de la información en las relaciones con los proveedores**		
A.15.1.1	Política de seguridad de la información sobre las relaciones con los proveedores	Si	Se debe de crear acuerdo de confidencialidad con cualquier entidad o proveedor externo que tenga acceso al sistema de informacion de la organización, en el cual se definen que tipo de acceso tendran que modificaciones se realizaran y las clausulas y penalidades de ley.

Continuacion Tabla 22			
A.15.1.2	Consideración de la seguridad en los acuerdos con los proveedores	NO	
A.15.1.3	Cadena de suministro de tecnología de la información y comunicación	NO	
A.15.2	**Gestión de la prestación del servicio por parte del proveedor**		
A.15.2.1	Monitoreo y revisión del servicio de los proveedores	NO	
A.15.2.2	Cambios en la gestión del servicio de los proveedores	NO	
A.16	**Gestión de los incidentes de seguridad de la información**		
A.16.1	**Gestión de los incidentes de la seguridad de la información y la mejora**		
A.16.1.1	Responsabilidades y procedimientos	NO	
A.16.1.2	Reporte de los eventos de seguridad de la información	NO	
A.16.1.3	Reporte de las debilidades de la seguridad de la información	NO	
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Si	Los eventos o incidentes presentados sobre los sistemas de informacion o equipos informaticos criticos deben estar debidamente documentados y de conocimiento por parte de los usuarios responsables, de esta forma poder tener un historial de fallas sobre los activos y poder diseñar planes de accion para evitar que se presenten.
A.16.1.5	Respuesta a los incidentes de seguridad de la información	NO	
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	NO	
A.16.1.7	Recolección de evidencia	NO	
A.17	**Gestión de los aspectos de la seguridad de la información para la continuidad del negocio**		
A.17.1	**Continuidad de la seguridad de la información**		
A.17.1.1	Continuidad de los planes de seguridad de la información	NO	

Continuacion Tabla 22			
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Si	Las politicas de seguridad sobre los activos de informacion deben estar debidamente documentadas y de conocimiento por parte de los responsables del proceso, de esta forma garantizar su continuidad y facilitar su mantenimiento.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Si	Las politicas de seguridad establecidas deben de evaluarse y actualizarse según los cambios que se puedan presentar en los sistemas de informacion o según la disposicion que contemple la gerencia o junta directiva sobre cambios de politicas gerenciales u objetivos de la organizacion.
A.17.2	**Redundancias**		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de la información	NO	
A.18	**Cumplimiento**		
A.18.1	**Cumplimiento de los requisitos legales y contractuales**		
A.18.1.1	Identificación de la ley aplicable y de los requisitos contractuales	NO	
A.18.1.2	Derechos de propiedad intelectuales	NO	
A.18.1.3	Protección registros	NO	
A.18.1.4	Privacidad y protección de la información que permite identificar a las personas	NO	
A.18.1.5	Regulación de los controles criptográficos	Si	Las politicas de cifrado sobre la informacion critica de la organización debe estar debidamente documentada, de conocimiento por parte del responsable del proceso y debe cumplir con los acuerdos, la legislacion y normativa pertinente.
A.18.2	**Revisiones de la seguridad de la información**		
A.18.2.1	Revisión independiente de la seguridad de la información	NO	
A.18.2.2	Cumplimiento de las políticas y normas de seguridad de la información	NO	
A.18.2.3	Revisión cumplimiento técnico	NO	

Fuente: William Salcedo Rodríguez basado en el anexo A de la Norma ISO 27001

12 CONCLUSIONES

El uso herramientas de auditoria forense, facilita la realización de pruebas pentesting sobre un ambiente controlado, de esta manera no afectar los activos ni detener los procesos en la organización estatal.

El uso de metodologías de análisis de riesgo Magerit, permite localizar las principales vulnerabilidades sobre el sistema de informacion y de esta manera facilitar el diseño de medidas de control y políticas de seguridad, basados en la norma ISO 270001, con el fin de mejorar y mantener el sistema de gestión de seguridad de la informacion.

Entre las vulnerabilidades encontradas, la principal amenaza radica en errores humanos ya sea de manera involuntaria o intencionalmente, de esta manera el tipo de ataque de ingeniera social debe de ser prevenido con políticas y planes de concientización sobre los usuarios internos de la organización estatal.

Las políticas y controles diseñados deben de ser reajustados continuamente, según las vulnerabilidades nuevas presentadas y los requisitos de seguridad requeridos por la organización.

13 RECOMENDACIONES

- Crear políticas de concientización hacia los usuarios, sobre buenas prácticas en el manejo de la información confidencial de la compañía, con el fin de evitar que se materialicen ataques de tipo ingeniería social.

- Implementación de políticas de seguridad más estrictas para el manejo de la información

- Desconfiar de mensajes sospechosos de remitentes desconocidos, con archivos adjuntos o que le siguieran seguir enlaces externos o descarga de archivos.

- Generar políticas de contraseñas de usuario robustas.

- Actualizar periódicamente los sistemas de antivirus y/o antimalware.

- Realizar Backups periódicamente de la información crítica.

14 BIBLIOGRAFÍA

AMUTIO Gómez, M. A., CANDAU, J., & Maña, J. A. (10 de 2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de Portal de Administración Electrónica.

B, G. (01 de 11 de 2019). *¿Qué es Apache? .* Recuperado el 26 de 04 de 2020, de Hostinger tutoriales: https://www.hostinger.co/tutoriales/que-es-apache/

Cano, J. J. (s.f.). *Colombia no está preparada ante un ciberataque.* Recuperado el 04 de 10 de 2020|, de Universidad del rosario.

Cano, J. J. (s.f.). *La ventana de AREM, estrategia para anticipar riesgos y amenazas.* Recuperado el 04 de 10 de 2020, de universidad del rosario.

DATA, D. (08 de Mayo de 2017). *El gobierno se suma al sector financiero y ocupa el primer puesto en la lista de objetivos de ataques cibernéticos.* Recuperado el 25 de 04 de 2020, de https://www.businesswire.com/news/home/20170507005010/es/

DE LUZ, S. (18 de 01 de 2014). *Redes Zone - Zenmap*. Recuperado el 26 de 04 de 2020, de cursodehackers.com: http://www.cursodehackers.com/nmap.html

DIGITAL GUIDES IONOS. (17 de 10 de 2016). *DIGITAL GUIDES IONOS.* Recuperado el 26 de 04 de 2020, de ¿En qué consiste una zona desmilitarizada (DMZ)?

DPL news. (10 de Junio de 2020). *Honda detiene su producción mundial tras un ataque de ransomware*. Obtenido de DPL News.

INCIBE. (25 de 04 de 2019). *INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD.* Recuperado el 26 de 04 de 2020

ISO 27001.ES. (s.f.). *SGSI*. Recuperado el 19 de 05 de 2020

Open Vas. (s.f.). *OpenVAS - Open Vulnerability Assessment Scanner*. Recuperado el 26 de 04 de 2020, de http://www.openvas.org/

REGISTRADURIA NACIONAL DEL ESTADO CIVIL. (s.f.). Recuperado el 26 de ABRIL de 2020, de https://www.registraduria.gov.co/-La-entidad-.html

RIVERO, M. (01 de 10 de 2016). *¿ Que son los Malwares ?* Recuperado el 2020 de 04 de 26, de infospyware.com: https://www.infospyware.com/articulos/que-son-los-malwares/

s.r.o., A. S. (s.f.). *¿Qué son los exploits?* Recuperado el 26 de 04 de 2020, de Avast.com: https://www.avast.com/es-es/c-exploits

Salcedo Rodriguez, W. E. (21 de Mayo de 2020). Presentacion Proyecto de Grado. Ibague: Youtube.

SENADO, S. (31 de 12 de 2019). *secretariasenado.gov.co.* Recuperado el 26 de 04 de 2020

Tamayo, J. (31 de 05 de 2017). *Empresas y entidades públicas colombianas también son víctimas de ataques de ransomware.* Obtenido de XATAKA Colombia.

tecnozero.com. (s.f.). *Zona DMZ*. Obtenido de tecnozero.com: https://www.tecnozero.com/blog/zona-dmz-zona-segura-contra-intrusos/

UNIVERSIDAD DE JAEN. (01 de 02 de 2018). *Guias de seguridad UJA - Ransomware.* Recuperado el 26 de 04 de 2020, de https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Triptico%20de%20seguridad%20UJA%20-%206.%20Ransomware.pdf

Wikipedia. (17 de 04 de 2020). *"Metasploit." Wikipedia, La enciclopedia libre.* Recuperado el 26 de 04 de 2020, de Wikipedia, La enciclopedia libre.: https://es.wikipedia.org/w/index.php?title=Metasploit&oldid=106627495

wikipedia.org. (s.f.). *Kali Linux*. Obtenido de wikipedia.org: https://es.wikipedia.org/w/index.php?title=Kali_Linux&oldid=112069535

15 ANEXOS

A continuacion se relacionan los anexos A y B.

15.1 Anexo A Video propuesta del proyecto

En el anexo A tenemos la presentación en video del proyecto como opción de grado, autor William Salcedo Rodroguez.

https://youtu.be/MClASzZkDzQ

Fuente: William Salcedo Rodríguez[21]

15.2 Anexo B Resumen RAE

En el anexo B tenemos el resumen analítico de educación – RAE, en el cual de manera corta se hace un análisis del proyecto como opción de grado de tal forma que facilite su interpretación.

Anexo B Resumen RAE

Fecha de Realización:	02/11/2020
Programa:	Especializacion en seguridad informatica
Línea de Investigación:	Infraestructura tecnologica y seguridad en redes
Título:	ANÁLISIS DE RIESGO SOBRE EL SISTEMA DE SEGURIDAD INFORMÁTICA DE UNA ENTIDAD ESTATAL COMO CASO DE ANÁLISIS SIMULADO EN UN AMBIENTE CONTROLADO
Autor(es):	Salcedo Rodriguez William Enrique
Palabras Claves:	Hackers, Defacement, Ransomware,SGSI, Salvaguardas
Descripción:	El presente proyecto se realizo como opción de grado de tipo proyecto aplicado en el área de Seguridad informática, el cual estudia el estado actual del SGSI de una entidad estatal como caso de análisis simulado en un ambiente controlado, esta entidad fue blanco de ataques por parte de Black Hackers, quienes materializaron ataques de tipo Defacement y Ransomware en las sedes de esta entidad en dos ciudades principales.

[21] Salcedo Rodriguez, William Enrique. «Presentacion Proyecto de Grado.» Ibague: Youtube, 21 de Mayo de 2020. https://www.youtube.com/watch?v=MClASzZkDzQ&feature=youtu.be.

	El objetivo principal es analizar los métodos de intrusión y proponer políticas y controles de seguridad que eviten la materialización de nuevos ataques.

Fuentes bibliográficas destacadas:

AMUTIO Gómez, M. A., CANDAU, J., & Maña, J. A. (10 de 2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Obtenido de Portal de Administración Electrónica.

B, G. (01 de 11 de 2019). *¿Qué es Apache? .* Recuperado el 26 de 04 de 2020, de Hostinger tutoriales: https://www.hostinger.co/tutoriales/que-es-apache/

Cano, J. J. (s.f.). *Colombia no está preparada ante un ciberataque.* Recuperado el 04 de 10 de 2020|, de Universidad del rosario.

Cano, J. J. (s.f.). *La ventana de AREM, estrategia para anticipar riesgos y amenazas.* Recuperado el 04 de 10 de 2020, de universidad del rosario.

DATA, D. (08 de Mayo de 2017). *El gobierno se suma al sector financiero y ocupa el primer puesto en la lista de objetivos de ataques cibernéticos.* Recuperado el 25 de 04 de 2020, de https://www.businesswire.com/news/home/20170507005010/es/

DE LUZ, S. (18 de 01 de 2014). *Redes Zone - Zenmap*. Recuperado el 26 de 04 de 2020, de cursodehackers.com: http://www.cursodehackers.com/nmap.html

DIGITAL GUIDES IONOS. (17 de 10 de 2016). *DIGITAL GUIDES IONOS.* Recuperado el 26 de 04 de 2020, de ¿En qué consiste una zona desmilitarizada (DMZ)?

DPL news. (10 de Junio de 2020). *Honda detiene su producción mundial tras un ataque de ransomware*. Obtenido de DPL News.

INCIBE. (25 de 04 de 2019). *INCIBE - INSTITUTO NACIONAL DE CIBERSEGURIDAD.* Recuperado el 26 de 04 de 2020

ISO 27001.ES. (s.f.). *SGSI*. Recuperado el 19 de 05 de 2020

Open Vas. (s.f.). *OpenVAS - Open Vulnerability Assessment Scanner*. Recuperado el 26 de 04 de 2020, de http://www.openvas.org/

REGISTRADURIA NACIONAL DEL ESTADO CIVIL. (s.f.). Recuperado el 26 de ABRIL de 2020, de https://www.registraduria.gov.co/-La-entidad-.html

RIVERO, M. (01 de 10 de 2016). *¿ Que son los Malwares ?* Recuperado el 2020 de 04 de 26, de infospyware.com: https://www.infospyware.com/articulos/que-son-los-malwares/

s.r.o., A. S. (s.f.). *¿Qué son los exploits?* Recuperado el 26 de 04 de 2020, de Avast.com: https://www.avast.com/es-es/c-exploits

Salcedo Rodriguez, W. E. (21 de Mayo de 2020). Presentacion Proyecto de Grado. Ibague: Youtube.

SENADO, S. (31 de 12 de 2019). *secretariasenado.gov.co.* Recuperado el 26 de 04 de 2020

Tamayo, J. (31 de 05 de 2017). *Empresas y entidades públicas colombianas también son víctimas de ataques de ransomware.* Obtenido de XATAKA Colombia.

tecnozero.com. (s.f.). *Zona DMZ*. Obtenido de tecnozero.com: https://www.tecnozero.com/blog/zona-dmz-zona-segura-contra-intrusos/

UNIVERSIDAD DE JAEN. (01 de 02 de 2018). *Guias de seguridad UJA - Ransomware.* Recuperado el 26 de 04 de 2020, de https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guiaspracticas/Triptico%20de%20seguridad%20UJA%20-%206.%20Ransomware.pdf

Wikipedia. (17 de 04 de 2020). *"Metasploit." Wikipedia, La enciclopedia libre.* Recuperado el 26 de 04 de 2020, de Wikipedia, La enciclopedia libre.: https://es.wikipedia.org/w/index.php?title=Metasploit&oldid=106627495

wikipedia.org. (s.f.). *Kali Linux*. Obtenido de wikipedia.org: https://es.wikipedia.org/w/index.php?title=Kali_Linux&oldid=112069535

Contenido del documento:	En el proyecto se Desarrolla una auditoría interna sobre el sistema de seguridad informático de una entidad estatal como caso de análisis simulado en un ambiente controlado, el cual requiere solución a un problema planteado acerca de dos ciberataques de tipo Defacement y Ransomware. **Objetivo general:** Diseñar las políticas para el control de seguridad informática que permita minimizar riesgos y materialización de nuevas amenazas de ataques, sobre el sistema informático de la entidad estatal en sus dos sedes principales.

Contenido del documento:	**Objetivos específicos:** • Realizar las pruebas de tipo pentesting haciendo uso de las herramientas de auditoria informática, en un ambiente controlado. • Simular los ataques de tipo Defacement y Ransomware, materializados por los Cyber delincuentes en la entidad estatal. • Realizar el inventario de activos e Identificación de las vulnerabilidades de seguridad presentes sobre los mismos, haciendo uso de la metodología MAGERIT. • Generar las políticas de seguridad y los controles necesarios según la norma ISO 27001 que den solución a las vulnerabilidades encontradas. Entre los principales capítulos que componen el documento tenemos: **Definicion del problema:** En el cual se realiza la presentación y formulación del problema. **Justificacion y Alcance:** En el cual definimos por que es necesario llevar a cabo la investigación y hasta que punto se llegara con la misma. **Marco Referencial:** En este capitulo tenemos en cuenta antescedentes a estudios o investigaciones previas sobre esta problemática, un marco contextual en el cual definimos el organigrama de la entidad, el marco teorico en el cual tenemos las bases o pilares que sustentan la investigación, es la parte fundamental de la investigación y sobre la cual nos apoyamos, tenemos un marco conceptual en la cual se definen términos claves dentro de la investigación, fienalmente esta el marco legal el cual indica bajo que normas, leyes o estatutos según la constitución colombiana y el COPNIA, nos podemos apoyar como fundamento para llevar a cabo la investigación. **Pruebas de Pentesting:** En este capitulo se hace uso de herramientas de informática forense como Kali Linux, Zen Map, OpenVAS, entre otras para realizar las pruebas de pentesting de tipo Black Box, ya que se tiene informacion básica de la entidad como es su topología de red y arquitectura de seguridad existente, pero siguiendo las

	características de un ataque externo, simulando los métodos de intrusión realizados en los ataques de tipo Defacement y Ransomware sobre la entidad estatal. **Diseño de controles y políticas de seguridad:** En este capitulo una vez identificados los métodos de instrusion por parte de los black Jackers, se diseñan los controles y políticas de seguridad siguiendo estas fases: • Identificacion de activos • Identificacion de amenazas y vulnerabilidades sobre los activos • Diseño de controles y políticas de seguridad
Marco Metodológico: **Marco Metodológico:**	Se hizo uso de la metodología MAGERIT en el análisis de riesgo sobre el sistema de informacion, esta metodología es muy útil debido a que nos permitio realizar de manera ordenada las siguientes fases: • Fase 1 identificación de activos. • Fase 2 identificación de amenazas y vulnerabilidades. • Fase 3 diseño de controles de seguridad Las salvaguardas están definidas por la norma ISO 27001, según la amenaza identificada, el tipo de tratamiento a implementar está definido por el método de gestión de riesgos MAGERIT.
Conceptos adquiridos :	El desarrollo de la investigación me permite apropiar de la mejor manera los conocimientos adqirirdos en el transcurso de la especialización en seguridad informática, con el objetivo de poder aplicarlos en un entorno real ya sea en ambiente laboral o como base para futuras investigaciones. Facilita enfrentarnos a problemáticas que conlleven la seguridad de la informacion, teniendo bases teóricas y experiencia que permitan soluccionarlos de la mejor manera. Finalmente complementa mis capacidades, aptitudes y experiencia como profesional en el area de sistemas y ahora especialista en seguridad informática.
Conclusiones:	El uso herramientas de auditoria forense, facilita la realización de pruebas pentesting sobre un ambiente

	controlado, de esta manera no afectar los activos ni detener los procesos en la organización estatal. El uso de metodologías de análisis de riesgo Magerit, permite localizar las principales vulnerabilidades sobre el sistema de informacion y de esta manera facilitar el diseño de medidas de control y políticas de seguridad, basados en la norma ISO 270001, con el fin de mejorar y mantener el sistema de gestión de seguridad de la informacion. Entre las vulnerabilidades encontradas, la principal amenaza radica en errores humanos ya sea de manera involuntaria o intencionalmente, de esta manera el tipo de ataque de ingeniera social debe de ser prevenido con políticas y planes de concientización sobre los usuarios internos de la organización estatal. Las políticas y controles diseñados deben de ser reajustados continuamente, según las vulnerabilidades nuevas presentadas y los requisitos de seguridad requeridos por la organización.