ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO DE UN PLAN DE MITIGACIÓN DE SEGURIDAD INFORMÁTICA A UNA RED INALÁMBRICA DE COMUNICACIÓN DE DATOS PARA UNA INSTITUCIÓN PRIVADA, A TRAVÉS DE LA APLICACIÓN DE HACKING ÉTICO PARA LA IDENTIFICACIÓN DE AMENAZAS, RIESGOS Y VULNERABILIDADES."

TRABAJO DE TITULACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SISTEMAS DE INFORMACIÓN GERENCIAL

Presentado por

ING. HUGO ARTURO PALTÁN ORELLANA

GUAYAQUIL - ECUADOR

AÑO 2018

AGRADECIMIENTO

Agradezco a nuestro Padre Jehová quien me ha brindado la salud y sabiduría para culminar con éxito este Trabajo de titulación.

A mi familia Milton, Rosa, Andrea y Carlos, por el apoyo incondicional en todo momento recibidos.

A la Institución para la cual se realizó este proyecto, por la apertura y las facilidades brindadas.

A mi tutora la Ing. Karina Astudillo, por su guía y experiencia en seguridad informática.

Finalmente agradezco a la Escuela Superior Politécnica del Litoral (ESPOL), en especial a quienes conforman el programa MSIG, por compartir sus conocimientos y experiencias formando en mí un profesional de alto nivel.

Hugo Paltán Orellana

DEDICATORIA

Dedico este trabajo a mi familia Milton, Rosa, Andrea y Carlos, por su confianza y apoyo incondicional.

A mis tíos Gonzalo y Susana por su ayuda y motivación para iniciar mis estudios de Postgrado.

A Fanny Paltán representante legal de la Institución para la cual se realizó el Trabajo de titulación.

A la Maestría en Sistemas de Información Gerencial (MSIG) y sus docentes por compartir sus conocimientos.

A todas aquellas personas, quienes con su inagotable paciencia y amor me brindaron su apoyo siempre.

Hugo Paltán Orellana

TRIBUNAL DE SUSTENTACIÓN

_____

Ing. Lenín Freire Cobo, MSIG

DIRECTOR MSIG

_____

Ing. Karina Astudillo Barahona, MBA

DIRECTOR DEL PROYECTO DE GRADUACIÓN

_____

Ing. Fabián Barboza Gilces, MSIA

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de Graduación de ESPOL)

_____

Ing. Hugo Arturo Paltán Orellana

RESUMEN

Las redes inalámbricas han ganado gran popularidad, ya que proporcionan a los usuarios el acceso a la información y los recursos en tiempo real, sin la necesidad de estar físicamente conectados. El objetivo de este trabajo de titulación es desarrollar un plan de mitigación de seguridad informática a una red inalámbrica de comunicación de datos, a través de la aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades.

Como guía utilizamos las metodologías: ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información), OWISAM (Metodología Abierta para el Análisis de Seguridad Wireless), y OSSTMM (Manual de la Metodología Abierta de Comprobación de la Seguridad). También aplicamos la Norma ISO/IEC 27002:2013, un estándar que proporciona recomendaciones sobre la gestión de seguridad inalámbrica.

Cabe destacar que el resultado obtenido de este trabajo permitió a la Institución identificar los niveles de riesgos de la red inalámbrica y aplicar un plan de mitigación, mejorando de manera importante aspectos como el control de acceso a los equipos físicos, la pérdida de información, la administración de políticas para el uso de la red inalámbrica y la gestión de dispositivos de comunicación; aumentando la confianza de los empleados.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

IEC	Comisión Electrónica Internacional.
ISO	Organización Internacional de Normalización.
ISO 27002	Estándar para la Seguridad de la Información.
ISSAF	Marco de Evaluación de Seguridad de Sistemas de Información.
OISSG	Seguridad de Sistemas de Información Abierto.
OSSTMM	Manual de la Metodología Abierta de Comprobación de la Seguridad.
OWISAM	Metodología Abierta para el Análisis de Seguridad Wireless.
WAP	Acceso Protegido Wifi.
WEP	Privacidad Equivalente al Cable.
WLAN	Red de Área Local Inalámbrica.
WMAN	Red de Área Metropolitana Inalámbrica.
WPAN	Red de Área Personal Inalámbrica.
WPS	Configuración de Wifi Segura.
WWAN	Red de Área Amplia Inalámbrica.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Las redes inalámbricas permiten la conexión de nodos sin la necesidad de utilizar medios físicos; ésta se transmite a través de ondas electromagnéticas bajo un protocolo de comunicación. Un usuario conectado a la red inalámbrica puede transmitir y recibir datos, voz y video dentro de edificios, entre edificios, en campus universitarios o incluso entre ciudades. Una de las principales ventajas es la disminución de los costos respecto a las redes cableadas, sin embargo, se tiene una considerable desventaja, derivada de la fácil vulnerabilidad en seguridad, que requiere la implementación de políticas y técnicas para evitar el ingreso a la infraestructura de la red.

Dentro de las redes inalámbricas se definen tres grupos distintos. El primer grupo se denomina WWAN o Redes de Área Amplia Inalámbrica, cuya potencia y alcance permiten abarcar grandes espacios e incluso ciudades. En el segundo grupo están las redes WLAN o Redes de Área Local Inalámbrica, y se caracterizan por su potencia y alcance medios, utilizados en entornos cerrados como edificios; estas redes están regidas por los estándares 802.11. En el tercer y último grupo se encuentran las redes WPAN o Redes de Área Personal Inalámbrica, que pertenecen a equipos que utilizan potencia reducida para cubrir espacios pequeños en el entorno de una oficina.

El presente trabajo tiene como propósito realizar un plan de mitigación de seguridad informática a una red inalámbrica de comunicación de datos, aplicando hacking ético para identificar amenazas, riesgos y vulnerabilidades. Este documento está dividido en 6 Capítulos estructurados de la siguiente manera:

En el Capítulo 1, se describen las generalidades del trabajo; los problemas existentes, sus objetivos generales y específicos, el alcance, la solución propuesta y la metodología. En el Capítulo 2, se presenta la fundamentación teórica de los elementos que conforman el proyecto.

Luego en el Capítulo 3, se realiza el levantamiento de información, identificando y seleccionando las metodologías y herramientas para la aplicación de hacking ético. Durante el Capítulo 4, se describe el análisis y evaluación de los riesgos; se inicia con la aplicación de pruebas intrusivas y no intrusivas. Todo este procedimiento se lleva a cabo en base a la metodología ISSAF y se integra con las metodologías OWISAM y OSSTMM. En el Capítulo 5, se desarrolla el plan de mitigación de riesgos y un análisis de factibilidad técnico, operativo y económico.

Finalmente, en el Capítulo 6, se analizan y comparan los resultados obtenidos con la realización del análisis de riesgos.

CAPÍTULO 1

GENERALIDADES

En este Capítulo se describen las generalidades del trabajo de titulación; los problemas existentes, sus objetivos generales y específicos, el alcance, la solución propuesta y la metodología.

1.1. Antecedentes

La cultura hacker data desde 1961, año en que el Instituto Tecnológico de Massachusetts (MIT) obtuvo el primer procesador de datos programado. El término “hacker” fue introducido a través del MIT. Los hackers del Tech Model Railroad Club (TMRC), se convirtieron en el

eje del laboratorio de inteligencia artificial del MIT; siendo el centro más importante de investigación sobre inteligencia artificial del mundo a principios de los 80. Luego de que su influencia se extendiera por todas partes desde 1969 se crea ARPANET; primera red intercontinental de alta velocidad y que fue fundada por el departamento de defensa estadounidense como un experimento de comunicaciones digitales. El término “hacker” se desarrolló en las universidades conectadas a la red, especialmente en sus departamentos de informática.

Existen dos términos hackers y crackers, cuyo significado es importante diferenciar. Los primeros son llamados sombrero blanco y su función es identificar fallas en los sistemas para luego informar al propietario y corregirlos. Los segundos son conocidos como sombrero negro, son piratas informáticos que ocupan sus capacidades para acciones ilegales.

La empresa sobre la cual se realizará el plan de mitigación de seguridad informática a su red inalámbrica, brinda servicios de viajes organizados, transporte y alojamiento, al público en general y también a empresas. Por temas de privacidad durante el proyecto se utilizará el término Institución para hacer referencia a la empresa.

1.2. Descripción del Problema

La Institución es una empresa familiar con sede en la ciudad de Guayaquil, establecida hace más de dos décadas y se dedica a brindar servicios de viajes organizados, transporte y alojamiento, al público en general y también a empresas. Cuenta con 2 sedes, cada una de ellas presenta una actividad principal distinta:

- **Sede 1:** Servicio de Viajes.
- **Sede 2:** Servicio de Alojamiento.

El trabajo de titulación se realizará sobre las 2 sedes antes mencionadas. Cada sede posee una infraestructura tecnológica independiente. La Institución dispone de un proveedor de internet para la Sede 1, siendo Grupo TV Cable con un Plan corporativo de 32Mbps. Mientras que en la Sede 2, su proveedor de internet es Netlife con un Plan de 20Mbps.

Los problemas que presenta la Institución fueron identificados a través de servicios de consultoría y soporte técnico a los equipos, aplicaciones y la infraestructura de red. También mediante de una entrevista técnica, con el objetivo de determinar la situación actual de la red inalámbrica se pudo identificar varios aspectos negativos.

Los problemas encontrados se detallan a continuación:

- **Falta de metodólogas de seguridad inalámbrica:** No se cuenta de metodologías para análisis, evaluación y comprobación del nivel de seguridad de la red inalámbrica.

- **Escases de pruebas de seguridad:** No se realizan pruebas periódicas a la red inalámbrica; que permitan encontrar amenazas y vulnerabilidades para reportarlas y tomar las medidas adecuadas.

- **Ausencia de análisis de riesgos:** No se efectúan estudios sobre análisis de riesgos, para evaluar peligros potenciales y virtuales consecuencias.

- **Falta de políticas de seguridad:** No se dispone de políticas de seguridad, acceso y uso de la red inalámbrica para los usuarios. Existe un control inadecuado de los recursos y servicios de la red.

- **Limitadas capacitaciones sobre herramientas de seguridad:** Se necesita de capacitaciones sobre seguridad informática y herramientas que podrían ser utilizadas por usuarios no autorizados para ingresar a la red y obtener información confidencial.

Particularidades Suscitadas:

Mediante un análisis realizado por un profesional en 2015, quien efectuó una consultoría de sistemas, pudo determinar una particularidad en la red inalámbrica. Cuando un cliente nuevo se registra en el Servicio de alojamiento, inmediatamente la administración le proporciona las contraseñas de las redes inalámbricas, y al conectarse a la red, tiene acceso a las cámaras de seguridad que monitorean las 24 horas. Aunque el acceso a las cámaras tiene protección por medio de contraseña, su configuración esta predeterminada de fábrica, lo que hace más fácil su intrusión. Las cámaras se encuentran conectadas al mismo segmento de la red que utilizan los clientes hospedados. Otro inconveniente que se presenta con frecuencia en la Institución es la interrupción del servicio de internet en la Sede 1 varias veces en un mismo día, lo que impide el correcto trabajo de los usuarios, clientes y administradores.

Riesgos:

Los riesgos relacionados con el acceso a la red inalámbrica son:

- Intercepción de los datos, escuchando transmisiones de varios usuarios de la red inalámbrica.

- Ataques de denegación de servicio, que podrían inutilizar la red al enviar solicitudes falsas.

- Pérdida y divulgación de información sensible para la Institución.

- Acceso no autorizado a la red inalámbrica.

1.3. Solución Propuesta

Después de analizar el problema se determinó que es necesario realizar un plan de mitigación, luego de aplicar hacking ético a la red inalámbrica de la Institución, usando herramientas de libre distribución y metodologías abiertas, tales como:

- Metodología ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información).

- Metodología OWISAM (Metodología Abierta para el Análisis de Seguridad Wireless).

- Metodología OSSTMM (Manual de la Metodología Abierta de Comprobación de la Seguridad).

Del mismo modo usaremos la Norma ISO/IEC 27002:2013, un estándar para la gestión de la seguridad de la Información.

A continuación, se detalla el uso de cada una de las metodologías:

- **Metodología ISSAF:** Se empleará para evaluar los controles de red y las aplicaciones; además para los formatos de la elaboración de reportes al cliente. Esta metodología se enfoca en 3 fases que se muestra en la Figura 1.1.

- **Metodología OWISAM:** Será utilizada para las pruebas y las recomendaciones de seguridad de la red inalámbrica.

- **Metodología OSSTMM:** Se usará para generar recomendaciones sobre auditoria de seguridad de los sistemas y los reportes.

- **Norma ISO/IEC 27002:2013:** Se usará para realizar el análisis de riesgos como parte del plan de mitigación, y proporcionar recomendaciones acerca de las mejores prácticas en la gestión de la seguridad de la información.

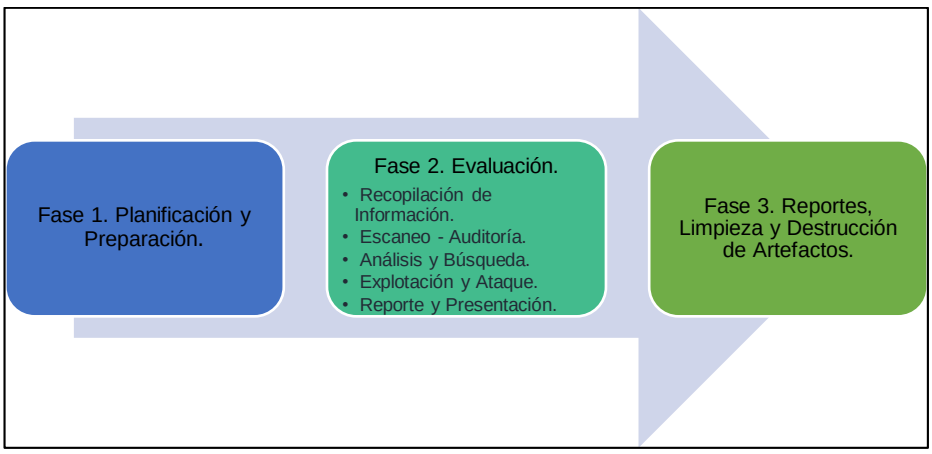


Figura 1.1: Metodología ISSAF

Fuente: Autoría Propia

Características de la Solución:

Las características de la solución sobre la cual se hará énfasis son:

- **Hacking Ético:** Se realizarán pruebas de intrusión y no intrusión a la red inalámbrica de la Institución, buscando amenazas y vulnerabilidades, que serán reportadas al cliente para tomar las medidas oportunas sin afectar el funcionamiento de la red.

- **Análisis y Evaluación de Riesgos:** Se determinará el impacto de los riesgos y su evaluación, para posteriormente elaborar un plan de mitigación.

- **Plan de Mitigación:** Este plan permitirá identificar las acciones que se deberán tomar frente al análisis de riesgos, reduciendo las amenazas y vulnerabilidades encontradas en la red.

- **Análisis de Factibilidad:** Se elaborará un análisis de tiempo, recursos, y costos. El análisis de factibilidad abordará los siguientes elementos:

    - Análisis Técnico: Se refiere a los recursos tangibles considerados para el plan de mitigación.

    - Análisis Económico: Hace referencia a los recursos económicos para elaborar el plan de mitigación y las pruebas.

- Análisis Operativo: Se refiere al proceso de analizar si el personal dispone de la experiencia técnica necesaria para ejecutar el plan de mitigación.

Beneficios:

Los principales beneficios que se lograrán con la aplicación de esta propuesta son:

- Mejora en los niveles de control de acceso físico a los equipos inalámbricos.
- Aplicación correcta de políticas de seguridad para uso de la red inalámbrica, a través de capacitaciones al personal de la Institución.
- Mejora en el nivel de seguridad de los dispositivos de comunicación, mediante el uso de contraseñas robustas, actualizaciones y control de inventario de equipos.
- Conocimiento del grado de vulnerabilidad de la red inalámbrica de la Institución, para aplicar las medidas de corrección.
- Reducción de los riesgos a través del plan de mitigación.

1.4. Alcance

- Se identificarán y aplicarán metodologías para hacking ético en la red inalámbrica.

- Se ejecutarán herramientas de software libre para escanear vulnerabilidades en la red de la institución.

- Se realizará un análisis, estimación y evaluación de riesgos; posteriormente se creará un plan de mitigación.

- Se elaborará un análisis comparativo de los resultados obtenidos con el análisis de riesgos antes y después del plan de mitigación.

1.5. Objetivo General

Desarrollar un plan de mitigación de seguridad informática a una red inalámbrica de comunicación de datos para una Institución privada, a través de la aplicación de hacking ético para la identificación de amenazas, riesgos y vulnerabilidades.

1.6. Objetivos Específicos

- Realizar el levantamiento de información e identificar y seleccionar las metodologías y herramientas para la aplicación de hacking ético de la red inalámbrica.

- Analizar y evaluar los riesgos de la red inalámbrica.
- Desarrollar el plan de mitigación de riesgos.
- Analizar y comparar los resultados obtenidos en la fase de análisis de riesgos con el plan de mitigación.

1.7. Metodología

La metodología a seguir presenta varios procesos que inician con: la definición del alcance del proyecto, la elaboración de un cronograma de trabajo, la recolección de datos a través de pruebas de seguridad, entrevistas y observación, la selección de las metodologías para la seguridad de las redes inalámbricas y las herramientas de hacking ético. Luego se continuará con el análisis, evaluación y tratamiento de riesgos, para posteriormente elaborar un plan de mitigación que será entregado, evaluado y aprobado como marco para la seguridad de la red inalámbrica de la Institución.

1.7.1. Población

Para la recolección de la información se definieron los sujetos más representativos del proyecto. La población está conformada por el Técnico de Redes y el Representante legal de la Institución; esto permitirá evaluar la red inalámbrica y analizar las expectativas desde el punto de vista administrativo.

1.7.2. Técnicas de Recolección de Datos

Las técnicas utilizadas para la recolección de datos son:

- **Entrevistas:** Se realizaron entrevistas al Técnico de Redes y al Representante Legal de la Institución, con el objetivo de conocer y determinar la situación actual de la red inalámbrica.

- **Observación:** Se observaron las instalaciones físicas, los usuarios, los servicios y aplicaciones, los equipos y dispositivos de la red inalámbrica. Además, se pudo observar todo el proceso de intrusión a la red con fines académicos.

El formato de la entrevista, se encuentra disponible mediante el **Anexo # 1.**

1.8. Recursos del Proyecto

Los recursos utilizados en el proyecto se clasifican en:

- **Recursos Humanos:** Se necesitó de un profesional de sistemas de información como Auditor de seguridad informática y un director de trabajo de titulación.

- **Recursos Tangibles:** Se utilizaron computadoras, una laptop, un adaptador de red Wifi USB, routers inalámbricos, dispositivos de almacenamiento, etc.

- **Recursos Intangibles:** Se usaron varias herramientas de software libre, sistemas y aplicativos que recomienda la metodología ISSAF para las pruebas de intrusión.

CAPÍTULO 2

MARCO TEÓRICO

En este Capítulo se presenta la fundamentación teórica de los elementos que conforman el proyecto.

2.1. Hacking Ético

El hacking ético permite analizar los sistemas y activos de información a través de pruebas de seguridad sobre la red de datos, con el objetivo de identificar amenazas, riesgos y vulnerabilidades; evaluando el estado actual de la organización para aplicar medidas correctivas.

De acuerdo a Astudillo K. (2013), hacking ético se define como:

> … la acción de efectuar pruebas de intrusión controladas sobre los sistemas, redes o dispositivos electrónicos; es decir el consultor o pentester, trabaja desde el punto de vista de un cracker, para encontrar vulnerabilidades en los equipos auditados, brindándole acceso al sistema afectado incluso; pero bajo un ambiente vigilado sin poner en riesgo la operatividad de los servicios informáticos de la organización cliente [1].

Cabe destacar que el consultor de seguridad informática debe poseer conocimientos avanzados sobre tecnología, poseer experiencia y seguir una metodología de trabajo certificada que permita optimizar los tiempos durante la fase de explotación.

2.2. Fases del Hacking

Es importante seguir un conjunto lógico de pasos durante la ejecución del servicio de hacking. Las fases de hacking se dividen en cinco y son descritas por eHack; empresa dedicada a brindar cursos, servicios y productos sobre seguridad informática. Las fases del hacker según eHack [2] siguen el siguiente orden:

"**Fase 1:** Reconocimiento, **Fase 2:** Escaneo, **Fase 3:** Obtener acceso, **Fase 4:** Mantener Acceso, **Fase 5:** Borrar huellas".

Mientras que el auditor informático que realiza un servicio de hacking ético tiene algunas fases similares, presenta variaciones a partir de la fase número 4 del hacking. Las fases del auditor de servicios informáticos por Astudillo K. [1] siguen el siguiente orden:

"**Fase 1:** Reconocimiento, **Fase 2:** Escaneo, **Fase 3:** Obtener acceso, **Fase 4:** Escribir Informe, **Fase 5:** Presentar Informe".

Todas estas fases forman parte de lo que se conoce como el círculo de hacking, que se ilustra en la Figura 2.1. Cabe descartar que el hacker ético es el encargado de escribir y presentar un informe con sus hallazgos y recomendaciones para aplicar los correctivos necesarios.

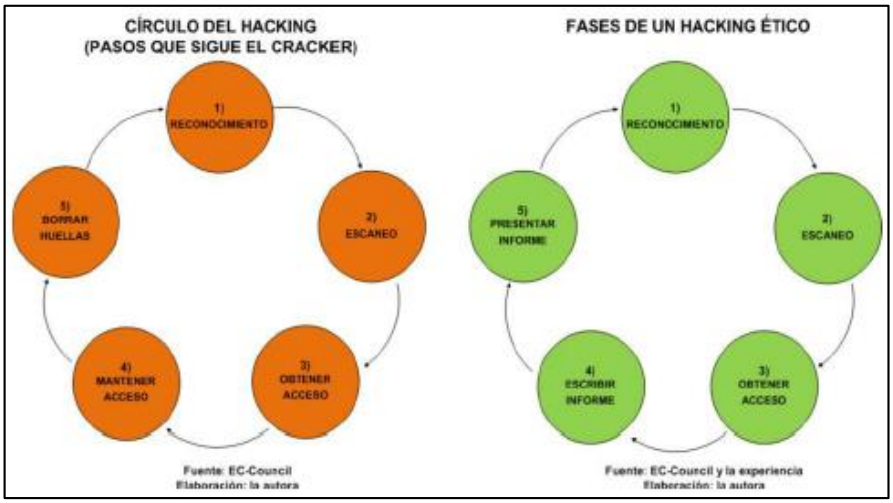


Figura 2.1: Fases de Hacking

Fuente: Astudillo, K. (2013). Fases de Hacking. [Figura]. Recuperado de https://www.amazon.com/Hacking-Etico-101-profesionalmente-Actualizada/dp/1535174064

2.3. Elementos de la Seguridad Informática

La seguridad informática representa un conjunto de medidas preventivas, de detección y corrección; que permiten resguardar y proteger la integridad y privacidad de los sistemas de información. Los elementos que conforman la seguridad informática, simbolizan los tres pilares fundamentales: integridad, confidencialidad y disponibilidad formando lo que se conoce como la tríada CIA de la seguridad informática mediante la Figura 2.2.

Figura 2.2: Triada CIA de la Seguridad Informática

Fuente: Mifsud, E. (2012). Introducción Seguridad. [Figura]. Recuperado de http://recursostic.educacion.es/observatorio/web/images/upload/elvira_mifsud/Introduccion_seguridad_html_6045ac9b.png

Según Benchimol D. (2011) en su Libro *Hacking desde Cero*, define los tres elementos de la seguridad informática [3]:

- **Confidencialidad**: Asegura que los usuarios (personas, procesos) no obtengan acceso a los datos a menos que estén autorizados.

- **Integridad:** Indica que toda la modificación de la información, sea realizada por usuarios debidamente autorizados.

- **Disponibilidad:** Garantiza que los recursos del sistema y la información estén disponibles únicamente para usuarios autorizados en el momento que los necesiten.

2.4. Políticas y Mecanismos de Seguridad Informática

Los profesionales que se ocupan de la seguridad informática deben tener en claro las políticas y mecanismos para la administración eficiente de los activos de la información. A continuación, se define cada uno de los términos:

- **Políticas de Seguridad:** Son una serie de lineamientos, reglas y normas que se deben seguir dentro de una organización para garantizar la seguridad de los activos de información. Para Borghello C. (2009), una política de seguridad se define como: “un conjunto de requisitos definidos por los responsables de un sistema, que indica en términos generales que está y que no está permitido en el área de seguridad durante la operación general del sistema” [4].

- **Mecanismos de Seguridad:** Son herramientas, métodos o procedimientos técnicos que se usan para cumplir las políticas y servicios de seguridad. Los mecanismos monitorean la información y los activos, previniendo la ocurrencia de un ataque informático. Los autores Ochoa y Cervantes (2012), en su artículo de investigación sobre *Seguridad Informática* definen un mecanismo de seguridad como: “técnicas que se utilizan para implementar un servicio, y están diseñados para detectar, prevenir o recobrarse de un ataque de seguridad” [5].

2.5. Tipos de Ataques de Hackers

Desde el punto de vista técnico existen varias formas en la que un atacante puede obtener acceso a un sistema. Los tipos de ataques de hackers señalados por Benchimol Daniel [3] son:

- **Ataques al Sistema Operativo:** Se centran en la búsqueda de errores sobre el sistema base de todo el resto del software, con el objetivo de controlar y explotar el sistema.

- **Ataques a las Aplicaciones:** Se toma en cuenta el uso masivo de las aplicaciones por parte de los usuarios. Las aplicaciones incrementan la probabilidad de ataque de un sistema, siendo recomendable evitar la instalación de aplicaciones innecesarias.

- **Ataques a las Configuraciones:** Las configuraciones tanto del sistema operativo como de las aplicaciones establecen un punto sensible, debido que un atacante podría aprovechar las configuraciones estándar de los equipos, dispositivos de red y aplicaciones, como vías de acceso.

- **Ataques a los Protocolos:** Los protocolos pueden presentar errores en su diseño, ocasionando un alto nivel de complejidad y problemas de seguridad, siendo necesario realizar modificaciones a distintos niveles para resolverlo, o ser reemplazado por otro más seguro.

Existe otro tipo de ataque denominado **Ingeniería Social**; que no hace uso de tecnología, sino más bien utiliza técnicas para manipular psicológicamente a las víctimas, con el propósito de obtener credenciales y vulnerar los sistemas de información.

En 2012, Jara y Pacheco [6] definieron la ingeniería social como: “la práctica para obtener datos confidenciales a través de la manipulación psicológica de usuarios legítimos”. Los ataques de ingeniería social pueden ser realizados por diversos canales como: por correo electrónico (phishing), por teléfono (vishing), a través de las redes sociales, mediante unidades externas como USB (baiting), y por mensaje de texto (smishing).

2.6. Modalidades del Hacking

Las modalidades del hacking dependen de la información proporcionada por parte del cliente hacia el auditor de seguridad informática. A menor información proporcionada, mayor será el tiempo invertido en investigar por parte del consultor. La Figura 2.3, presenta las tres modalidades del servicio de hacking: Black Box Hacking, Grey Box Hacking y White Box Hacking.

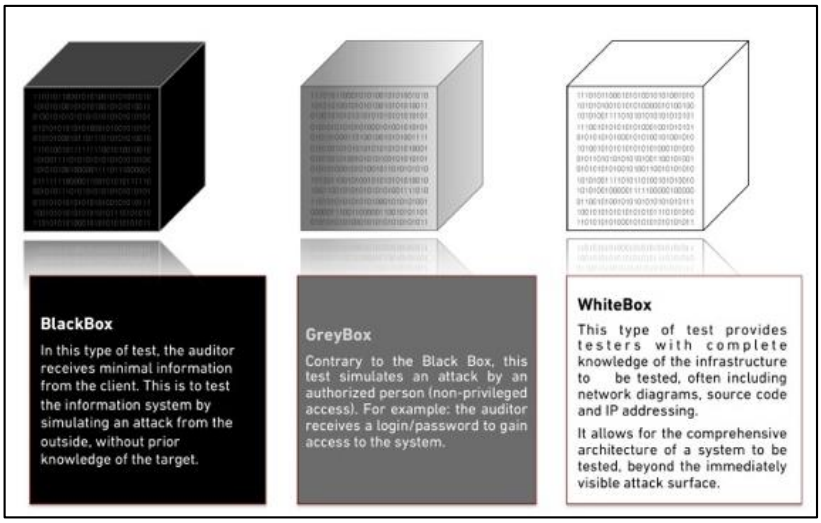


Figura 2.3: Modalidades del Hacking

Fuente: SecuLabs. (2018). Penetration Test. [Figura]. Recuperado de https://www.seculabs.ch/img/black-box.jpeg

Astudillo K. (2013), lista y describe las modalidades del servicio de hacking [1] como:

- **Black Box Hacking:** Llamado hacking de caja negra, se utiliza en pruebas de intrusión externas. El cliente proporciona poca

información al consultor, siendo la organización una caja negra para él. Se requiere mayor tiempo y por ende su costo es superior.

- **Grey Box Hacking:** Llamado hacking de caja gris, suele utilizarse para referirse a las pruebas de intrusión internas y en ocasiones a pruebas externas, donde el cliente proporciona información técnica sobre los equipos públicos y sistemas a ser auditados.

- **White Box Hacking:** Llamado hacking de caja blanca, ésta modalidad se aplica a pruebas de intrusión internas exclusivamente, donde la empresa cliente proporciona información completa al consultor sobre las redes y sistemas a auditar.

2.7. Metodología ISSAF

La metodología ISSAF o *Marco de Evaluación de la Seguridad de Sistemas de Información*, es un proyecto producido por el Grupo de Seguridad de Sistemas de Información Abierto (OISSG). Es un marco organizado de análisis de seguridad de la información; que presenta lineamientos para realizar pruebas de seguridad inalámbrica. El propósito de esta metodología es evaluar la red, sistemas y aplicaciones. Se enfoca en tres fases y nueve pasos de evaluación.

Fases de la Metodología ISSAF:

De acuerdo con la metodología ISSAF [7], existen tres fases:

- **Fase 1 (Planificación y Preparación):** Para SCProgress (2017), empresa de Seguridad Informática *Servicios Computacionales Progress*, esta fase establece: “el intercambio de información, planificación y preparación para la prueba de evaluación. Se deberá firmar previamente un acuerdo entre ambas partes. Se definirá la contribución del equipo, tiempos de pruebas, fechas, privilegios, etc.” [8]. Las actividades ejecutadas dentro de esta fase son:

  - Identificación de las personas del contacto.

  - Reunión para puntualizar el enfoque, la metodología, y el alcance en función a los casos de pruebas, la progresión de rutas y privilegios.

- **Fase 2 (Evaluación):** Durante esta fase se lleva a cabo las pruebas de penetración. Está dividida en nueve capas como se muestra en la Figura 2.4, y son:

  - **Capa 1:** Recolección de información.

- **Capa 2:** Mapeo de la red de trabajo.
- **Capa 3:** Identificación de vulnerabilidades.
- **Capa 4:** Penetración.
- **Capa 5:** Obtener acceso y escalada de privilegios.
- **Capa 6:** Enumeración.
- **Capa 7:** Comprometer usuarios remotos y sitios.
- **Capa 8:** Mantener acceso.
- **Capa 9:** Cubrir rastros.

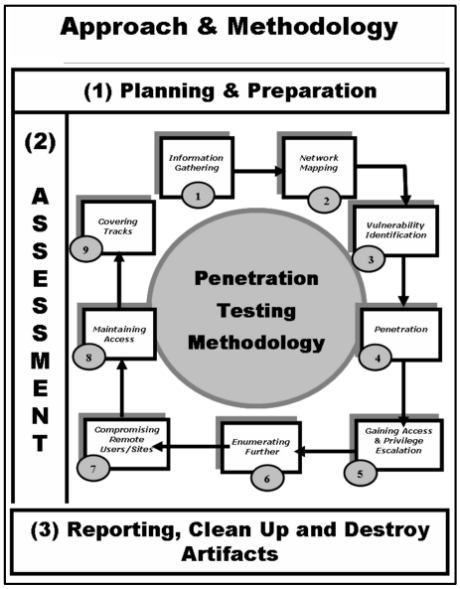


Figura 2.4: Capas de la Fase Evaluación

Fuente: ISSAF. (2005). Enfoque y Metodología ISSAF. [Figura]. Recuperado de https://www.oissg.org/files/issaf0.2.1A.pdf

- **Fase 3 (Reporte, Limpieza y Destrucción):** Para SCProgress (2017), en esta fase: “se presenta reportes. Durante las pruebas de penetración y de presentarse un evento crítico, se deberá informar inmediatamente para garantizar la continuidad de la organización. En este punto se deben discutir y buscar contramedidas para resolver problemas críticos” [8]. Terminadas las pruebas, se crea un informe técnico con la descripción de los resultados y las recomendaciones. Los elementos que se deben incluir en el informe son:

  - Resumen.
  - Alcance del proyecto.
  - Herramientas.
  - Fechas y horas de realización de las pruebas.

2.8. Metodología OWISAM

La metodología OWISAM o *Metodología de Evaluación de Seguridad Wireless Abierta*, surge con el objetivo de crear controles de seguridad, que se deben verificar sobre las redes de comunicación inalámbricas y que ayudan a los administradores de redes, sistemas y analistas de seguridad informática a identificar riesgos y minimizar

el impacto de los ataques informáticos; garantizando la protección de las infraestructuras inalámbricas basadas en el estándar 802.11.

Fases de la Metodología OWISAM:

La metodología OWISAM no dispone de una estructura para realizar pruebas de penetración; sin embargo, presenta una serie de controles con un listado de verificaciones técnicas. La Figura 2.5, ilustra la secuencia de las fases de la metodología OWISAM.

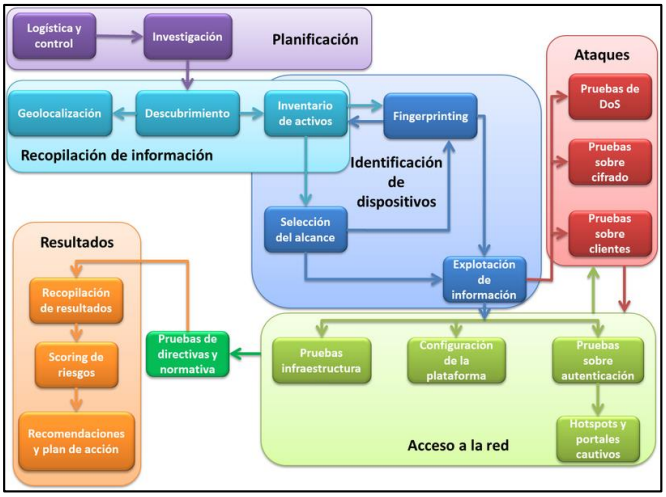


Figura 2.5: Fases de la Metodología OWISAM

Fuente: TARLOGIC. (2017). Controles de Metodología OWISAM. [Figura]. Recuperado de https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/

De acuerdo a la metodología OWISAM [9], existen siete fases:

- **Fase 1:** Planificación.
- **Fase 2:** Recopilación de información.

- **Fase 3:** Identificación de dispositivos.
- **Fase 4:** Ataques.
- **Fase 5:** Acceso a la red.
- **Fase 6:** Pruebas sobre normativa y directivas.
- **Fase 7:** Generación de resultados.

Controles OWISAM:

Los controles OWISAM presentan secciones que guían las mejores prácticas, para estudiar el riesgo al que se encuentra expuesta la red inalámbrica de la Institución. La Tabla 1, presenta un resumen de los controles OWISAM organizados en 10 secciones.

Tabla 1: Lista de Controles OWISAM

#	Sección	Referencia	Control
1	Descubrimiento	OWISAM-DI	Descubrimiento de información de redes inalámbricas.
2	Fingerprinting	OWISAM-FP	Análisis de las funcionalidades soportadas por los dispositivos.
3	Pruebas sobre la autenticación	OWISAM-AU	Examen de los mecanismos de autenticación Wifi.

4	Pruebas de cifrado de las comunicaciones	OWISAM-CP	Estudio de los mecanismos de cifrado de información.
5	Pruebas de configuración de la plataforma	OWISAM-CF	Verificación de la configuración de las redes.
6	Análisis de infraestructura	OWISAM-IF	Revisiones de seguridad sobre la infraestructura inalámbrica.
7	Denegación de servicio	OWISAM-DS	Verificación de la disponibilidad de los servicios.
8	Pruebas sobre directivas y normativa.	OWISAM-GD	Análisis de normativas sobre el uso de las redes de Wifi.
9	Pruebas sobre clientes inalámbricos	OWISAM-CT	Ataques contra clientes inalámbricos.
10	Pruebas sobre Hostspots/portales cautivos	OWISAM-HS	Debilidades que afectan al uso de portales cautivos.

Fuente: Nota. Recuperado de Auditoría Wireless - Auditoría de seguridad Wifi OWISAM. Copyright 2017 por la Empresa Tarlogic.

La lista completa de los controles OWISAM se encuentran disponibles en el **Anexo # 2.**

2.9. Metodología OSSTMM

La metodología OSSTMM o *Manual de la Metodología Abierta de Comprobación de la Seguridad*, es un estándar que presenta un marco de trabajo basado en secciones; y comúnmente es utilizado en auditorias de seguridad para la revisión de los sistemas.

Secciones de la Metodología OSSTMM:

Mediante la Figura 2.6 es posible observar el mapa de seguridad OSSTMM; donde la parte resaltada en color amarillo corresponde al conjunto de seguridad inalámbrica.

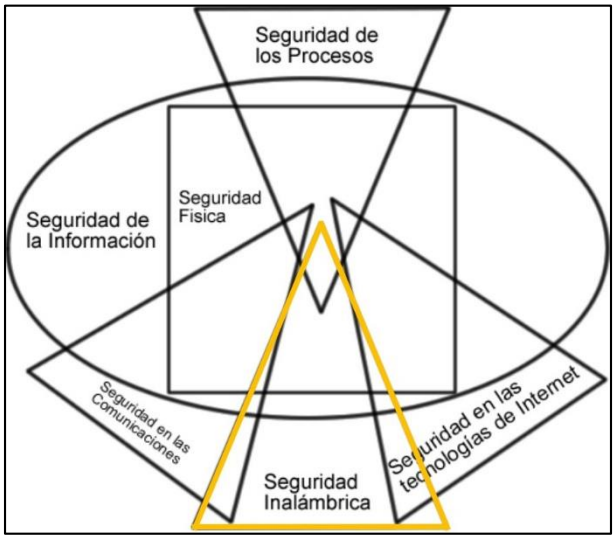


Figura 2.6: Mapa de Seguridad OSSTMM

Fuente: ISECOM. (2003). Mapa de Seguridad OSSTMM. [Figura]. Recuperado de http://www.isecom.org/research/osstmm.html

Según la metodología OSSTMM [10], ésta consta de 6 secciones:

- **Sección A:** Seguridad de la Información.
- **Sección B:** Seguridad de los Procesos.
- **Sección C:** Seguridad en las Tecnologías de Internet.
- **Sección D:** Seguridad en las Comunicaciones.

- **Sección E:** Seguridad Inalámbrica.

- **Sección F:** Seguridad Física.

La lista completa de los módulos del mapa de seguridad OSSTMM están disponibles en el **Anexo # 3.**

Estructura de Pruebas y Tareas OSSTMM:

Las secciones de la metodología OSSTMM se sobreponen entre sí, y representan las áreas concretas sobre la cual se realizará el análisis de seguridad. Los módulos constituyen el flujo de la metodología desde un punto de seguridad hacia otro. Un módulo posee una entrada (información usada en el desarrollo de cada tarea) y una salida (resultado de las tareas completadas). La Figura 2.7, muestra un ejemplo de un módulo para pruebas y tareas OSSTMM.

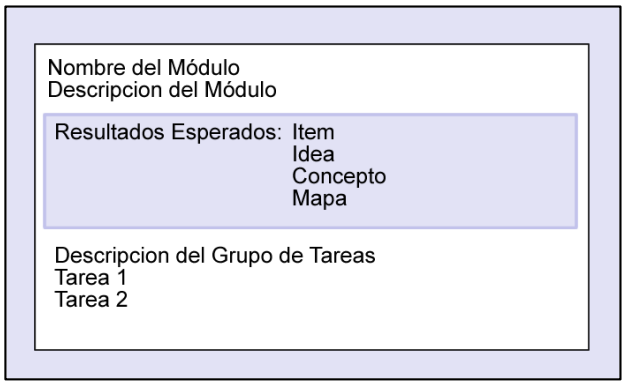


Figura 2.7: Estructura de Pruebas y Tareas OSSTMM

Fuente: ISECOM. (2003). Módulos de Test y Tareas. [Figura]. Recuperado de http://www.isecom.org/research/osstmm.html

2.10. Norma ISO/IEC 27002:2013

Es un estándar para la seguridad de la información, creado por la *Organización Internacional de la Normalización* (ISO) y la *Comisión Electrónica Internacional* (IEC). Ésta norma recomienda las mejores prácticas en la gestión de seguridad de la información a todos los profesionales responsables en iniciar, implementar o mantener sistemas de gestión de la seguridad de la información.

Directrices ISO/IEC 27002:2013:

De acuerdo a la norma ISO/IEC 27002:2013 [11], constan 14 dominios principales:

- **Dominio 1:** Políticas de Seguridad.
- **Dominio 2:** Organización de la Seguridad de la Información.
- **Dominio 3:** Seguridad de Recursos Humanos.
- **Dominio 4:** Gestión de Activos.
- **Dominio 5:** Control de Accesos.
- **Dominio 6:** Cifrado.
- **Dominio 7:** Seguridad Física y Ambiental.

- **Dominio 8:** Seguridad de las Operaciones.
- **Dominio 9:** Seguridad de las Telecomunicaciones.
- **Dominio 10:** Adquisición, desarrollo y mantenimiento de los sistemas de información.
- **Dominio 11:** Relaciones con los Proveedores.
- **Dominio 12:** Gestión de Incidentes en la Seguridad de la Información.
- **Dominio 13:** Aspectos de Seguridad de la Información para la Administración de la Continuación del Negocio.
- **Dominio 14:** Cumplimiento.

La lista completa de los 14 dominios, 35 objetos de control y 114 controles; se encuentra disponible en el **Anexo # 4.**

2.11. Herramientas para Pruebas de Seguridad

Son un conjunto de aplicaciones que permiten detectar y recopilar información de routers o puntos de accesos inalámbricos; comprobando el nivel de seguridad de la red. Ayudan a remediar y reducir las posibilidades de sufrir ataques en la red de la organización.

Las principales herramientas para pruebas de seguridad Wifi son:

- **Ubuntu:** Es una distribución GNU/Linux, se comercializa como software libre y está orientado al usuario promedio. Para Benchimol D. (2011), Ubuntu es: “un sistema operativo fácil, sencillo de utilizar y de instalar, muchas de sus innovaciones en materia de software y usabilidad son tomadas para desarrollar e incorporarlos en nuevos proyectos” [12].

- **Kali Linux:** Es una distribución GNU/Linux, dirigida a pruebas de penetración y auditoría de seguridad. De acuerdo a *Offensive Security* (2018), éste sistema contiene herramientas que están orientadas a: “diversas tareas de seguridad de la información, pruebas de penetración, investigación de seguridad, informática forense e ingeniería inversa” [13].

- **NMAP (Network Mapper):** Es un programa de código abierto que permite ver los equipos activos en la red, y escanear los puertos para posteriormente realizar ataques. Según NMAP, en su guía de referencia utiliza: “paquetes IP originales para determinar qué equipos se encuentren disponibles en la red, los servicios que ofrecen, los sistemas operativos que ejecutan, los tipos de filtros de paquetes, entre otras” [14].

- **Wireshark:** Es un analizador de protocolos de código abierto, utilizado para el análisis del tráfico y resolución de problemas de red. Wireshark [15] implementa: “una amplia gama de filtros que facilitan la definición de criterios de búsqueda para los más de 1100 protocolos soportados actualmente, por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados”.

- **Suite Aircrack-ng:** Es un paquete completo de herramientas para evaluar la seguridad de la red Wifi, y se ejecuta sobre la línea de comandos CMD. Las áreas sobre las cuales se centra Aircrack-ng [16] son: “monitoreo o captura de paquetes, ataques, des-autentificación, puntos de acceso falsos, pruebas de comprobación de tarjetas Wifi, cracking WEP y WPA”.

- **Acrylic Wifi:** Es un sniffer gratuito desarrollado por *Tarlogic Security SL*, permite monitorear las redes inalámbricas y comprobar su nivel de seguridad. Según Tarlogic, entre los objetivos de esta aplicación constan: “identificar las redes inalámbricas, determinar los canales y SSID, coleccionar las direcciones IP y MAC de un access point, determinar el método de encriptación de un access point, entre otros” [17].

- **Vistumbler:** Es un programa que permite escanear las redes wifi y proporciona información de las conexiones disponibles. Incluye soporte para GPS.

- **Wifi Analyzer:** Es una aplicación gratuita disponible en Google Play, que permite analizar y verificar la calidad de la señal; y el nivel de saturación de cada red.

2.12. Redes Inalámbricas y Tipos

Son redes que se comunican usando medios no guiados como ondas electromagnéticas, microondas o infrarrojo. La transmisión y recepción se efectúa a través de antenas. La Figura 2.8, ilustra las diferentes tecnologías de redes inalámbricas, que se distinguen por la frecuencia, el alcance y la velocidad de transmisión.

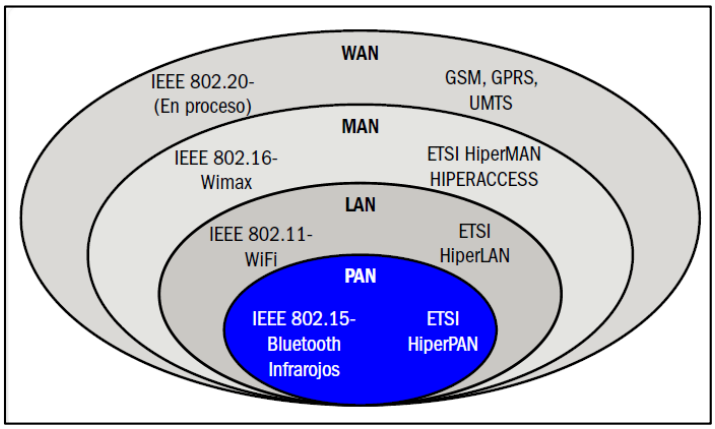


Figura 2.8: Estándares para Redes Inalámbricas

Fuente: Carballeiro, G. (2012). Tecnologías Inalámbricas y sus Estándares. [Figura]. Recuperado de https://www.amazon.com.mx/Redes-Wi-Fi-Entornos-Windows/dp/9871857640

Tipos de Redes Inalámbricas:

Para Andreu J. (2011), las redes inalámbricas [18] se clasifican según su alcance y/o tecnología en:

- **WPAN:** *Red de área personal inalámbrica*, es una red de interconexión de periféricos que se pueden encontrar tanto a pocos centímetros como a metros de distancia del emisor. Los estándares más conocidos son el bluetooth y el infrarrojo.

- **WLAN:** *Red de área local inalámbrica*, es una red que puede situarse en el mismo edificio con un óptimo de 100m y hasta un máximo de 450m. La más conocida es Wifi con el estándar 802.11.

- **WMAN:** *Red de área metropolitana inalámbrica*, es una red que se sitúa en un barrio, urbanización o municipio pequeño. Las tecnologías de este grupo se conocen como inalámbricas de banca ancha (WiMax o WiBro), que soportan hasta 54km de distancia en condiciones favorables y 22km en condiciones climatologías adversas.

- **WWAN:** *Red de área amplia inalámbrica*, es una red basada en tecnólogas vSAT (Terminal de Apertura Muy Pequeña), para conexiones satelitales usadas en barrios, capitales, campo, etc. Las tecnologías más conocidas son para telefonía móvil, GPRS, GSM, 2G/3G/4G, etc.

2.13. Tipos de Cifrado en Redes Inalámbricas

Se denomina cifrado al procedimiento que utiliza un algoritmo con clave para transformar un mensaje; de tal manera que sea difícil de comprender a quienes no dispongan de dicha clave secreta.

Valdivia C. (2005) en su libro *Sistemas informáticos y redes locales,* analiza los diferentes tipos de cifrados [19] para las redes inalámbricas:

- **WEP:** *Privacidad Equivalente al Cableado*, es un sistema de cifrado pensado para proporcionar una confidencialidad igual a la de una red cableada tradicional. Provee un cifrado en la capa 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 o 128 bits.

- **WPA:** *Acceso Protegido Wifi*, es un sistema de cifrado basado en las especificaciones del estándar IEEE 802.11i, que mejora el nivel de protección de los datos y el control de acceso a las redes inalámbricas. Utiliza el algoritmo RC4 con una clave de 128 bits. Implementa un Protocolo de Integridad de Clave Temporal (TKIP), que cambia claves dinámicamente a medida que el sistema es utilizado.

- **WPA 2:** *Acceso Protegido Wifi 2*, es un sistema que protege las redes wifi. Introducido para corregir las deficiencias detectadas en WPA. Los puntos de acceso del protocolo WPA 2 utilizan el algoritmo AES (Estándar de Cifrado Avanzado). AES es un sistema de cifrado por bloques con claves de 128, 192, 256 bits; que lo convierte en un sistema más seguro.

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACÍON, METODOLOGÍAS, Y HERRAMIENTAS PARA HACKING ÉTICO

En este Capítulo se realiza el levantamiento de información, se identifica y seleccionan las metodologías y herramientas de software libre para la aplicación de hacking ético de la red inalámbrica.

3.1. Caracterización de la Red de la Institución

La Institución dispone de dos sedes ubicadas en la ciudad de Guayaquil. La Sede 1, se encarga de los servicios de viajes; mientras que la Sede 2, se dedica a brindar servicios de alojamiento. Cada área

posee una infraestructura tecnológica independiente. La Sede 1, cuenta con un proveedor de internet que es Grupo TV Cable con un Plan corporativo de 32Mbps. Mientras que en la Sede 2, su proveedor de internet es Netlife con un Plan de 20Mbps.

Usuarios de la Red:

Los usuarios que acceden diariamente a la red de la Institución en sus dos sedes son 33 aproximadamente. Estos usuarios son de tipo administrativo, empleados y clientes especificando:

- Sede 1 (Servicio de Viajes): 8 usuarios.
- Sede 2 (Servicio de Alojamiento): 25 usuarios.

Servicios Funcionales de la Red:

Los servicios que disponen los usuarios por medio del acceso a la red inalámbrica son: correo electrónico empresarial, cámaras de seguridad, internet y soporte a usuarios. La Institución habitualmente accede a diversas aplicaciones para realizar pagos, transferencias bancarias, envío y recepción de correos, reservaciones, declaración de obligaciones tributarias, pagos de seguro de empleados, consultas de programas turísticos, etc.

Activos de la Red:

La Institución posee una infraestructura cableada e inalámbrica, que permite compartir archivos, acceder a servicios y aplicaciones de manera fácil. Dentro del proyecto se analizarán los dispositivos detallados en la Tabla 2, que corresponden a las 2 sedes.

Tabla 2: Activos de Red de la Institución

Sede	Cantidad	Equipo	Marca	Descripción
Alojamiento	1	Módem	Motorola Sb5101	Brindar acceso a Internet.
	2	Router Wifi	D-Link DIR -615	Compartir inalámbricamente la conexión a Internet.
	1	Switch	D-Link DES -105	Brindar conexión a las computadores, puntos de acceso inalámbrico, cámaras IP, etc.
	1	DVR	Avtech AVC792C 4 Canales	Ofrecer video vigilancia a distancia de las Instalaciones en tiempo real.
	3	Tarjeta de Red Inalámbrica	QPCOM QP-W5400NPCI	Compartir información y recursos entre 2 o más equipos inalámbricamente.
Viajes	1	Router Wifi	QPCOM	Compartir inalámbricamente la conexión a Internet.
	1	Televisor	Smart TV	Monitorear las cámaras de seguridad.

Fuente: Autoría Propia

Diagrama de Red:

La Figura 3.1, muestra el diagrama de red de las sedes de alojamiento y de viajes. Esta red presenta una topología de tipo estrella, y como medio de transmisión para de la red LAN utilizan cable par trenzado categoría 6. Las sedes no se encuentran conectadas entre sí por un enlace WAN; sin embargo, comparten información por medio de Internet. El área de alojamiento posee cámaras de video vigilancia que son monitoreadas remotamente. Los servicios web y de correo electrónico son provistos por una empresa externa.

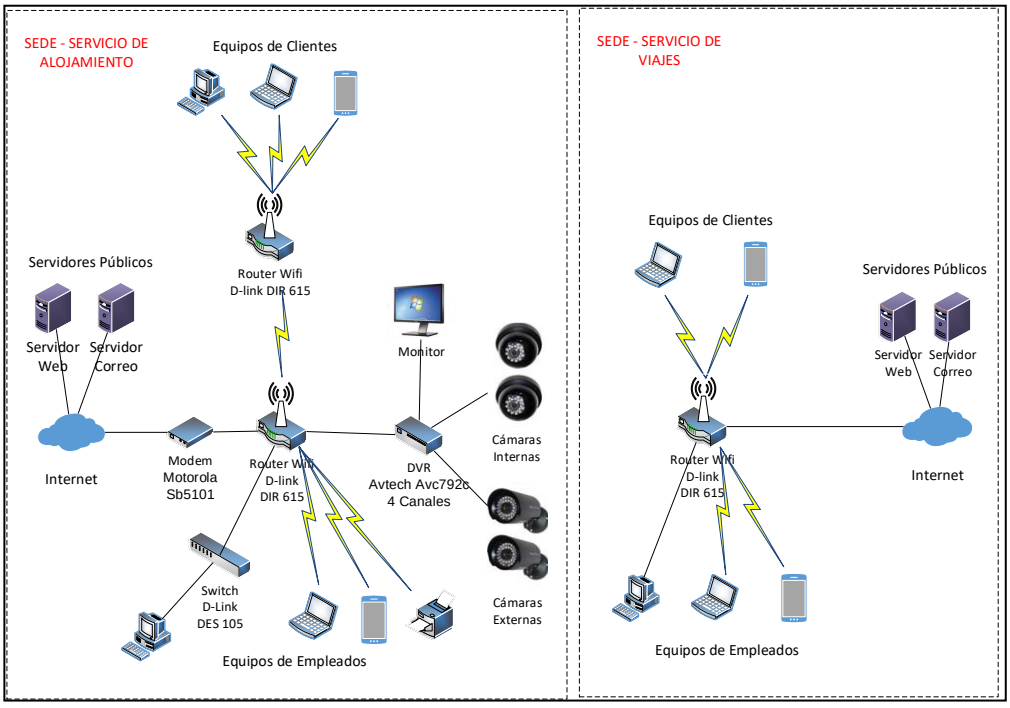


Figura 3.1: Diagrama de Red de la Institución

Fuente: Autoría Propia

3.2. Selección de las Metodologías de Seguridad Inalámbrica

Las metodologías y normas consideradas en este proyecto son:

- **Metodología ISSAF:** Será la guía principal. Seguiremos como referencia su versión Draft 0.2 en la *Sección M*, que corresponde a la *"Evaluación de la Seguridad WLAN"*. Las fases de ésta sección son: recopilación de información, escaneo – auditoria, análisis y búsqueda, explotación y ataque, reporte y presentación.

- **Metodología OWISAM:** Se usarán varios controles de la metodología OWISAM como: descubrimiento e identificación de dispositivos, pruebas de autenticación, pruebas de cifrado, pruebas de configuración de plataforma, análisis de infraestructura, pruebas sobre directivas y normativa, etc.

- **Metodología OSSTMM:** Será utilizada como guía la *Sección E - Seguridad Inalámbrica*. Dentro de esta sección nos centraremos en el apartado número 2 que corresponde a la *"Verificación de Redes Inalámbricas (802.11)".*

Cabe destacar que haremos uso también de la **Norma ISO/IEC 27002:2013**; para la elaboración del plan de mitigación, proporcionando recomendaciones de las mejores prácticas de la gestión de seguridad de la información.

3.3. Selección de las Herramientas de Hacking Ético

Las herramientas de hacking ético para este proyecto deberán cumplir ciertos aspectos como: ser de libre distribución, permitir la detección e identificación de redes inalámbricas, aplicar auditoría de la seguridad informática, ser de fácil instalación en máquinas virtuales, disponer de gran documentación técnica sobre su instalación y configuración, etc. La Tabla 3, clasifica las herramientas utilizadas en cada una de las subfases de la metodología ISSAF.

Tabla 3: Herramientas para Hacking Ético

SubFase ISSAF	Herramienta
Recopilación de Información	Acrylic Wifi, Vistumbler, Wifi Analyzer, Aircrack-ng.
Escaneo - Auditoría	Ubuntu, Acrylic Wifi, Vistumbler, Wifi Analyzer, Advanced IP Scanner, NMAP, CMD.
Análisis y Búsqueda	Acrylic Wifi, Wireshark, Aircrack-ng.
Explotación y Ataque	Kali Linux, Wireshark.
Reporte y Presentación	Kali Linux.

Fuente: Autoría Propia

3.4. Identificación de Amenazas en la Red Wifi

Una amenaza es una posibilidad de ocurrencia de un evento o acción que tiene el potencial de causar daño sobre los elementos de un sistema informático. La Tabla 4, contiene las amenazas más comunes en una red inalámbrica.

Tabla 4: Amenazas más Comunes en Redes Wifi

No	Amenaza
1	Acceso No Autorizado
2	Daños por agua
3	Escuchas encubiertas
4	Espionaje
5	Fallas de políticas de seguridad inalámbrica
6	Falla en la seguridad de la comunicación
7	Fraude
8	Fuego
9	Mala configuración de la red inalámbrica
10	Inadecuado mantenimiento de la red inalámbrica
11	Ingeniería social
12	Intercepción de la información
13	Robo común
14	Virus

Fuente: Autoría Propia

3.5. Probabilidad de Ocurrencia de Amenaza

La probabilidad de ocurrencia revela la frecuencia en que puede ocurrir o materializarse una amenaza. Los criterios para estimar la probabilidad de ocurrencia se muestran en la Tabla 5.

Tabla 5: Criterios para Estimar la Probabilidad de Ocurrencia

Probabilidad	Valor	Descripción
Muy Baja	**1**	Se puede materializar 1 vez cada 3 o 5 años.
Baja	**2**	Se puede materializar 1 vez cada 2 años.
Media	**3**	Se puede materializar 1 vez cada año.
Alta	**4**	Se puede materializar 1 vez cada mes.
Muy Alta	**5**	Se puede materializar 1 vez cada semana.

Fuente: Autoría Propia

CAPÍTULO 4

ANÁLISIS, EVALUACIÓN Y TRATAMIENTO DE RIESGOS

En este Capítulo se describe el análisis, evaluación y tratamiento de riesgos, comienza con la aplicación de pruebas de seguridad sobre la red inalámbrica.

4.1. Aplicación de Pruebas de Penetración

Para la aplicación de las pruebas de penetración es indispensable utilizar los lineamientos de la metodología ISSAF; que será la guía

principal en el desarrollo del proyecto. Las fases y sus tareas a realizar son:

- **Fase 1 (Planeación y Preparación):** Realizando tareas como la definición del alcance del servicio y la planificación de actividades a través de un cronograma de trabajo.

- **Fase 2 (Evaluación):** Ejecutando las pruebas de seguridad en la red inalámbrica.

- **Fase 3 (Reportes, Limpieza y Destrucción de Artefactos):** Presentando un reporte de los resultados obtenidos al técnico de la red y representante de la Institución. Incluye también la limpieza y la destrucción de los objetos obtenidos.

4.2. Fase 1: Planeación y Preparación

Durante esta fase se llevará a cabo dos tareas: el alcance del servicio de hacking ético, y la planificación de las actividades.

Alcance del Servicio:

El alcance del servicio establece:

- El proyecto se ejecutará sobre las sedes de transporte y alojamiento de la Institución.

- Las pruebas de penetración son de tipo intrusivas y no intrusivas.
- La modalidad del servicio de hacking es de caja gris.
- Durante los horarios de oficina se aplicarán las pruebas de seguridad.
- Las pruebas serán ejecutadas desde el interior a la Institución.

Planificación de Actividades:

Las actividades a realizar siguen las 3 fases de la metodología ISSAF antes mencionadas. Las pruebas de penetración se ubican sobre la *Fase 2: Evaluación*. Por tal razón, es importante elaborar un cronograma de actividades que permita llevar un control de los tiempos asignados para cada tarea como lo muestra la Tabla 6.

Tabla 6: Planificación de Actividades

	Enero				Febrero				Marzo			
Actividad	1	2	3	4	1	2	3	4	1	2	3	4
F1: Planificación y Preparación												
F2: Evaluación												
- Recopilación de Información												
- Escaneo - Auditoría												
- Análisis y Búsqueda												
- Explotación y Ataque												
F3: Reportes, Limpieza y Destrucción de Artefactos												

Fuente: Autoría Propia

4.3. Fase 2: Evaluación

Durante esta fase se realizarán las pruebas de penetración en la red inalámbrica de la Institución. Ésta fase a su vez presenta varias subfases sobre la red WLAN que son: Recopilación de Información, Escaneo - Auditoría, Análisis y Búsqueda, Explotación y Ataque, Reporte y Presentación. Podemos diferenciar los dos tipos de ataques que se aplican durante la ejecución de las pruebas:

- **Ataques Pasivos:** El atacante únicamente escucha el flujo de tráfico para obtener información transmitida, pero no altera la comunicación.

- **Ataques Activos**: El atacante modifica el flujo de datos para ocasionar efectos en la red.

Identificación de Pruebas de Seguridad:

Tomando como referencia las secciones de los controles OWISAM, y luego de analizar los problemas encontrados; se identificaron las pruebas de seguridad a realizar siguiendo las subfases de la metodología ISSAF para WLAN. También fue de gran importancia asociar las herramientas de hacking ético y su modo de ataque, como lo muestra la Tabla 7.

Tabla 7: Identificación de Pruebas de Seguridad Inalámbrica

SubFase ISSAF	Pruebas/Controles OWISAM	Herramientas	Modo Ataque
Recopilación Información	Descubrimiento activo de dispositivos y redes. **(OWISAM-DI-005)**	• Acrylic Wifi Professional.	Pasivo
Escaneo	Identificación de funcionalidades soportadas por el dispositivo. **(OWISAM-FP-002)**	• Vistumbler. • Wireshark.	Pasivo
Auditoría	Pruebas sobre WPS. **(OWISAM-AU-002)**	• Acrylic Wifi Professional.	Pasivo
	Interfaces administrativas expuestas a la red. **(OWISAM-IF-002)**	• Advanced IP Scanner.	Pasivo
	Prueba de Traceroute	• Consola de Windows. • Zenmap.	Activo
	Prueba de AP/Router	• Zenmap.	Activo
	Análisis de configuración de dispositivos. **(OWISAM-GD-004)**	• Cuestionario.	Pasivo
	Análisis de la política de gestión y cambio de claves. **(OWISAM-GD-005)**	• Cuestionario.	Pasivo
	Verificación de inventario de dispositivos autorizados. **(OWISAM-GD-006)**	• Cuestionario.	Pasivo
Análisis y Búsqueda	Verificación del nivel de intensidad de señal o área de cobertura. **(OWISAM-CF-003)**	• Wifi Analyzer. • Acrylic Wifi Professional.	Pasivo
	Debilidades en el firmware del AP. **(OWISAM-IF-001)**	• Observación.	Pasivo
	Análisis de protocolos de cifrado inseguro (WEP, TKIP) **(OWISAM-CP-004)**	• Kali Linux	Activo

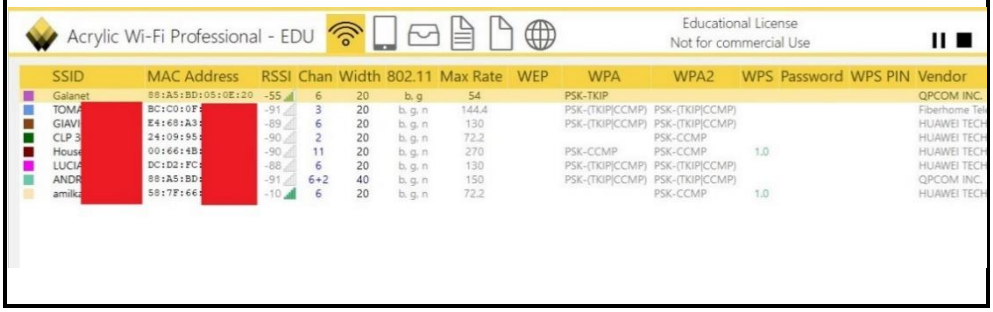
Explotación y Ataque	Captura y cracking de claves transmitidas en el proceso de autenticación. **(OWISAM-AU-004)**	• Kali Linux	Activo
	Pruebas de deautenticación. **(OWISAM-DS-001)**	• Kali Linux	Activo

Fuente: Autoría Propia

4.4. Ejecución de Pruebas

La ejecución de las pruebas de seguridad es documentada utilizando una plantilla sugerida por la norma ISSAF. Las pruebas constan desde la Tabla 8 hasta la Tabla 21.

Tabla 8: Prueba de Descubrimiento de Dispositivos y Redes

Prueba 1. Descubrimiento activo de dispositivos y redes.
Objetivos
Descubrir información de los dispositivos y la red inalámbrica de la Institución.
Pre-requisitos
• Instalar Acrylic Wifi Professional.
Ejemplos/Resultados
SEDE #1 - Servicio de Viajes


SEDE #2 - Servicio de Alojamiento

Análisis/Conclusión/Observación

La Sede 1, presenta un sistema de autenticación WPA y encriptación (PSK-TKIP). La Sede 2, dispone del mecanismo de seguridad WPS.

Contramedidas

Revisar el Plan de Mitigación de Riesgos.

Enlaces

ISSAF:

- http://www.oissg.org/issaf.html

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/

SOFTWARE:

- https://www.acrylicwifi.com/

Herramientas

- Acrylic Wifi Professional EDU v3.2

Observaciones

- **Subfase de Metodología ISSAF:** Recolección de información.
- **Control OWISAM:** OWISAM Discovery.
- **Subcontrol OWISAM:** Descubrimiento activo de dispositivos y redes (OWISAM-DI-005).
- **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

Tabla 9: Prueba de Funcionalidades Soportadas por el Dispositivo

Prueba 2. Identificación de funcionalidades soportadas por el dispositivo.

Objetivos

Conseguir información sobre los dispositivos de comunicación inalámbrica (software y hardware).

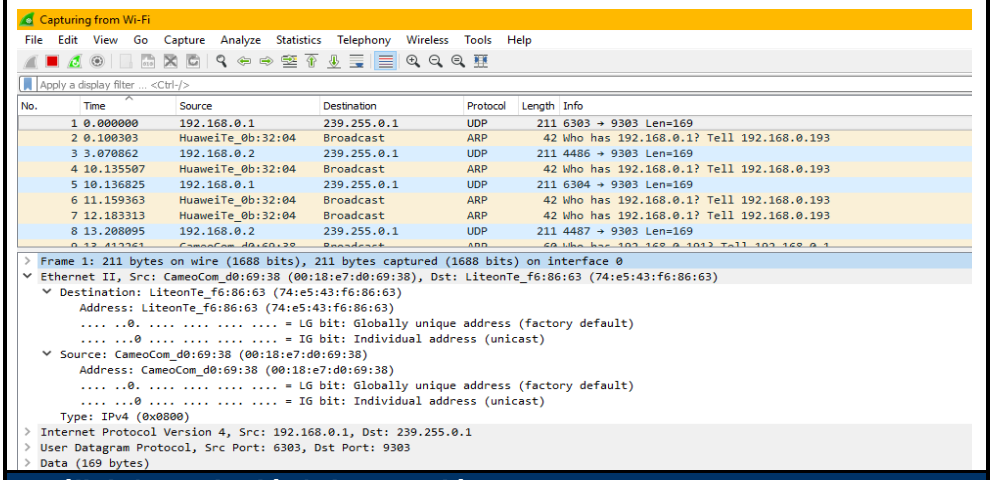
Pre-requisitos

- Instalar Vistumbler.
- Instalar Wireshark.

Ejemplos/Resultados

SEDE #1 - Servicio de Viajes

SEDE #2 - Servicio de Alojamiento



Análisis/Conclusión/Observación

Se pudo obtener información de ambas sedes tales como: fabricante, dirección MAC, SSID, autenticación, encriptación, señal, etc.

Contramedidas

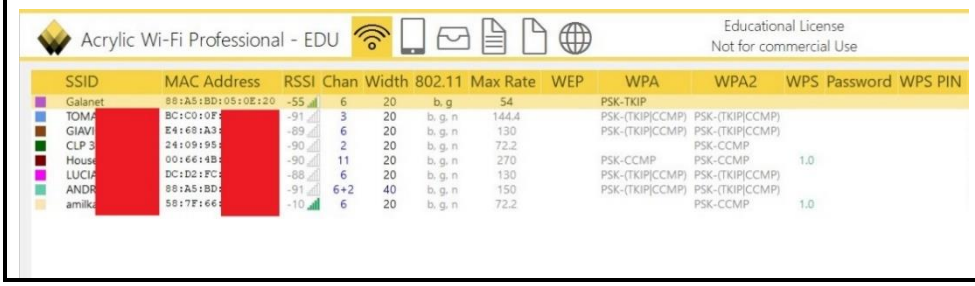
Revisar el Plan de Mitigación de Riesgos.

Enlaces

ISSAF: • http://www.oissg.org/issaf.html OWISAM: • https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx • https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/ • https://auditoriawifi.es/controles-owisam/ SOFTWARE: • https://www.vistumbler.net/ • https://www.wireshark.org/
Herramientas
• Vistumbler v10.6 • Wireshark v2.4
Observaciones
• **Subfase de Metodología ISSAF:** Escaneo. • **Control OWISAM:** OWISAM Fingerprinting. • **Subcontrol OWISAM:** Identificación de funcionalidades soportadas por el dispositivo (OWISAM-FP-002). • **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

Tabla 10: Prueba sobre WPS

Prueba 3. Pruebas sobre WPS.
Objetivos
Verificar si los dispositivos tienen activado el protocolo WPS.
Pre-requisitos
• Instalar Acrylic Wifi Professional.
Ejemplos/Resultados
SEDE #1 - Servicio de Viajes 

SEDE #2 - Servicio de Alojamiento

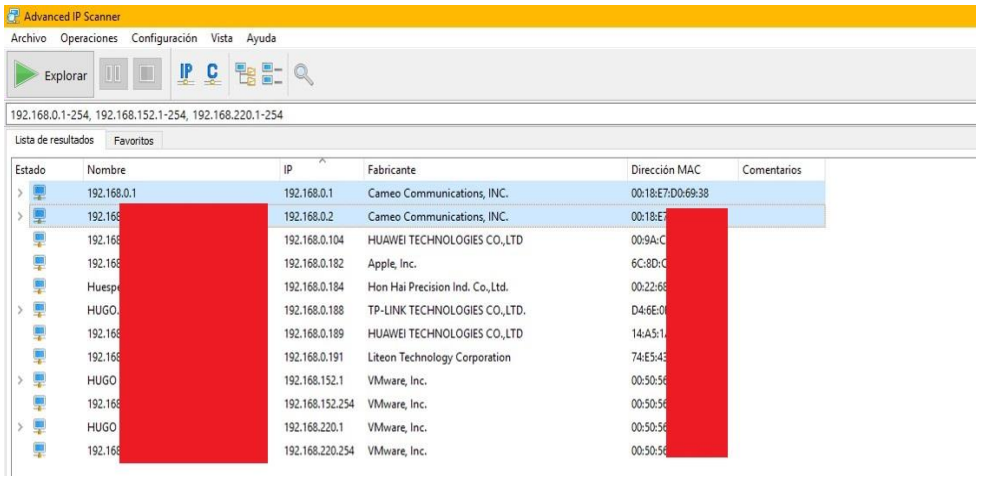
Análisis/Conclusión/Observación
Únicamente la Sede 2 tiene habilitado el protocolo WPS.
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces
ISSAF: • http://www.oissg.org/issaf.html OWISAM: • https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx • https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/ • https://auditoriawifi.es/controles-owisam/ SOFTWARE: • https://www.acrylicwifi.com/
Herramientas
• Instalar Acrylic Wifi Professional - EDU v3.2
Observaciones
• **Subfase de Metodología ISSAF:** Auditoria. • **Control OWISAM:** Pruebas sobre la autenticación. • **Subcontrol OWISAM:** Pruebas sobre WPS (OWISAM-AU-002). • **Modo de Ataque:** Pasivo.

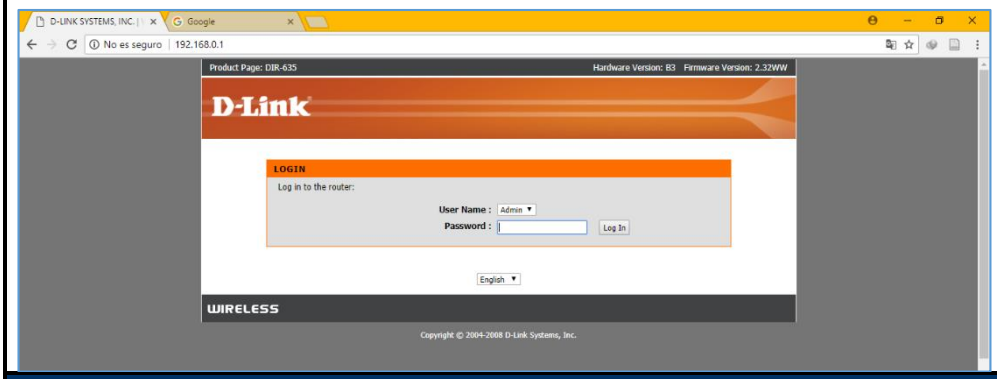
Fuente: Autoría Propia

Tabla 11: Prueba de Interfaces Administrativas Expuestas a la Red

Prueba 4. Interfaces administrativas expuestas a la red.
Objetivos
Escanear e identificar el acceso a la gestión de los dispositivos inalámbricos en la Institución.
Pre-requisitos
• Instalar Advanced IP Scanner.
Ejemplos/Resultados

SEDE #2 - Servicio de Alojamiento





Análisis/Conclusión/Observación

Se puede administrar los dispositivos inalámbricos desde su puerta de enlace y con las credenciales predeterminadas de fábrica.

Contramedidas

Revisar el Plan de Mitigación de Riesgos.

Enlaces

ISSAF:

- http://www.oissg.org/issaf.html

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/
- https://auditoriawifi.es/controles-owisam/

SOFTWARE:

- https://www.advanced-ip-scanner.com/es/

Herramientas

- Advanced IP Scanner v2.5

Observaciones

- **Subfase de Metodología ISSAF:** Auditoria.

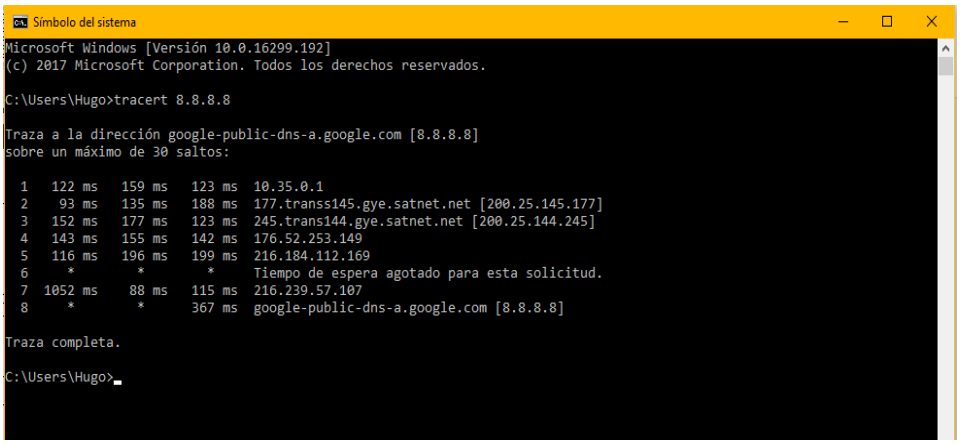
- **Control OWISAM:** Análisis de Infraestructura.
- **Subcontrol OWISAM:** Interfaces administrativas expuestas a la red (OWISAM-IF-002).
- **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

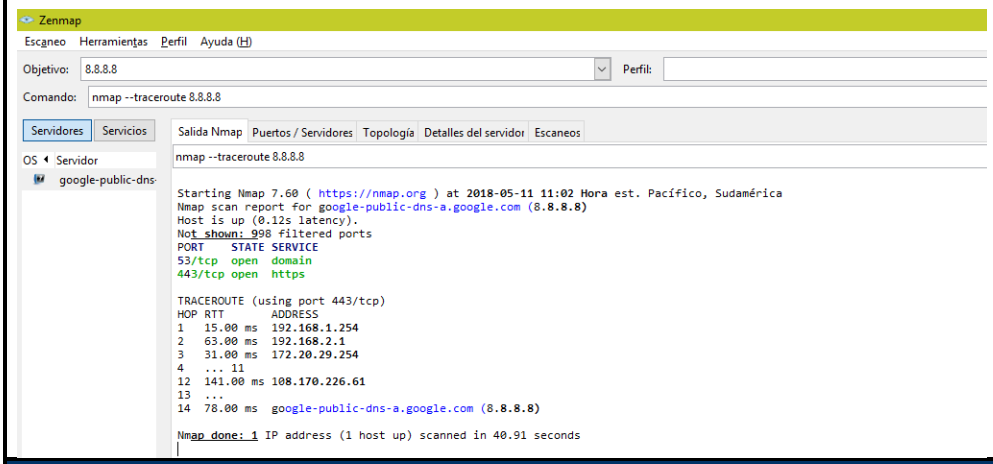
Tabla 12: Prueba de Traceroute

Prueba 5. Prueba de Traceroute
Objetivos
Diagnosticar la pista de los paquetes que vienen desde un punto de red.
Pre-requisitos
• Consola de Windows. • Instalar Zenmap.
Ejemplos/Resultados

SEDE #1 - Servicio de Viajes



SEDE #2 - Servicio de Alojamiento



Análisis/Conclusión/Observación
Se pudo constatar la estadística RTT (latencia de red) de los paquetes transmitidos en cada salto.
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces
ISSAF: • http://www.oissg.org/issaf.html SOFTWARE: • https://nmap.org/zenmap/
Herramientas
• Zenmap v7.6 • Consola de Windows
Observaciones
• **Subfase de Metodología ISSAF:** Auditoria. • **Modo de Ataque:** Activo.

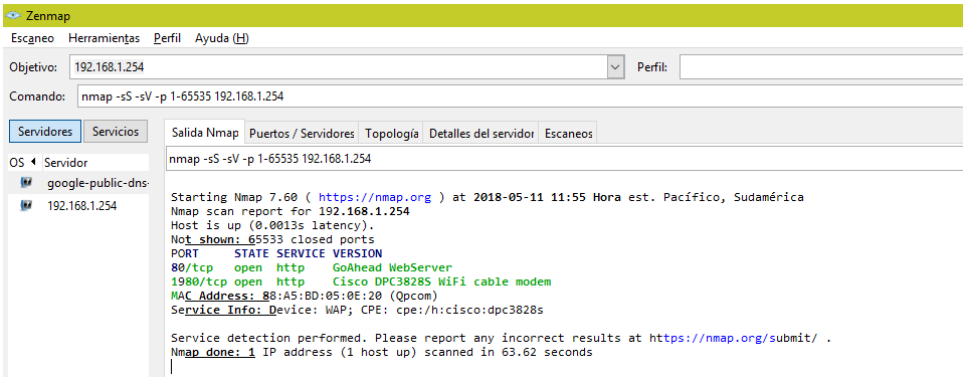
Fuente: Autoría Propia

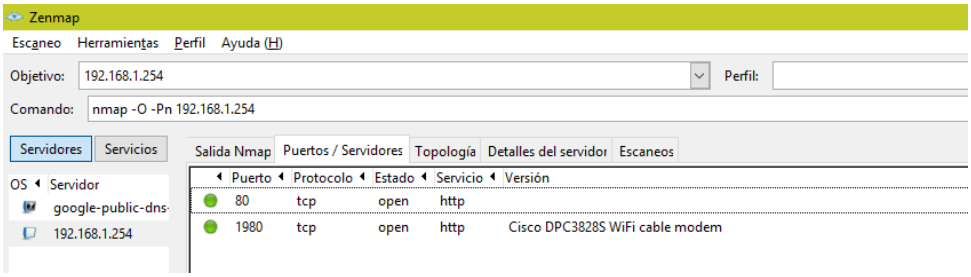
Tabla 13: Prueba de APs/Router

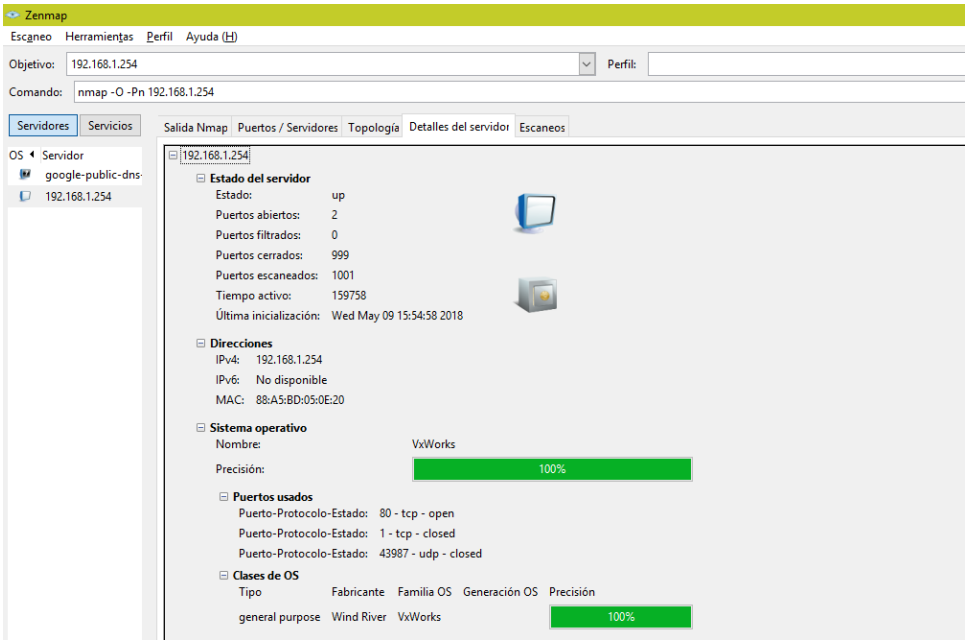
Prueba 6. Prueba de APs/Router
Objetivos
Identificar los puertos, protocolos y servicios de enrutamiento que estén abiertos.
Pre-requisitos
• Instalar Zenmap.

Ejemplos/Resultados

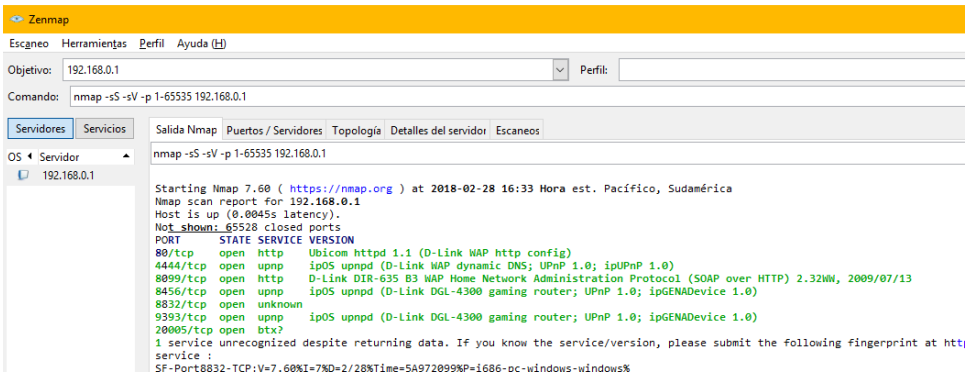
SEDE #1 - Servicio de Viajes

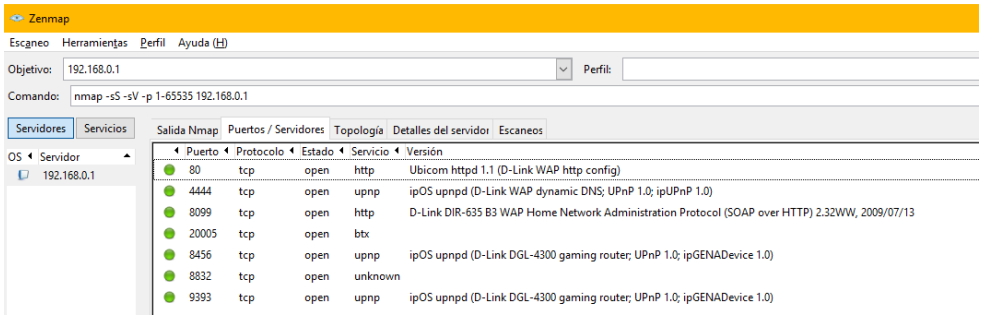


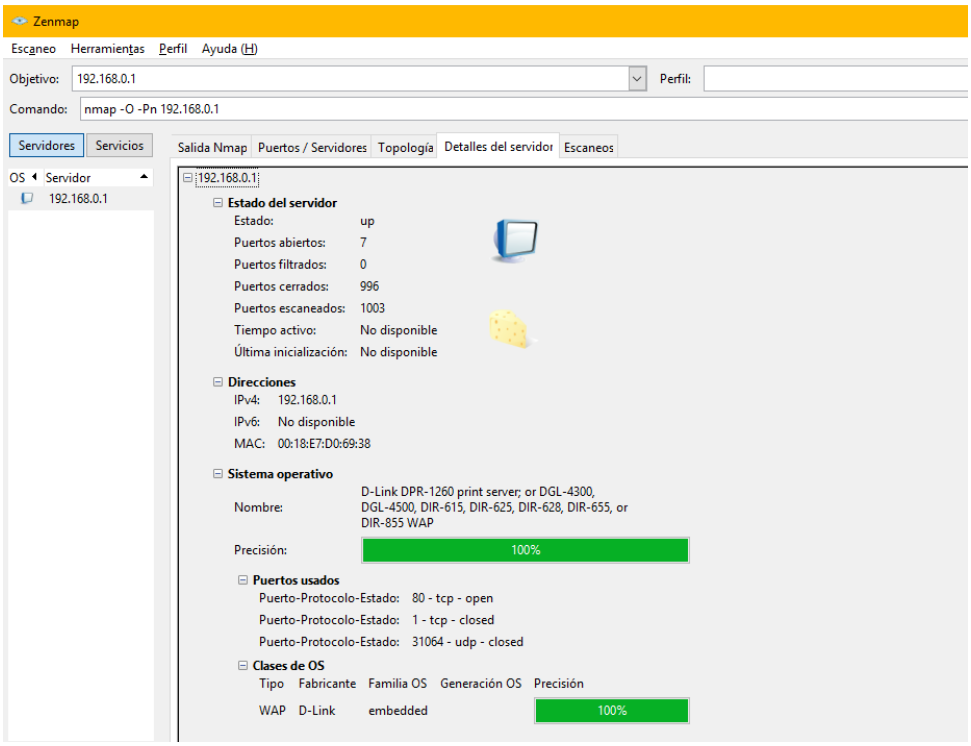




SEDE #2 - Servicio de Alojamiento







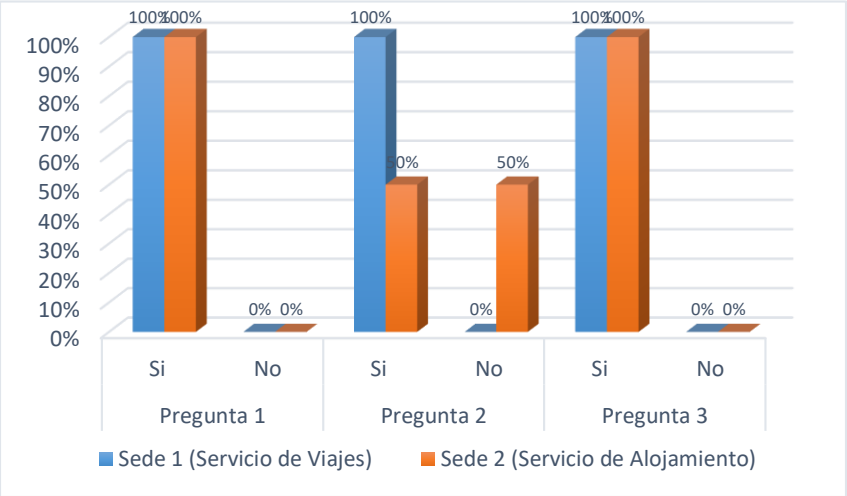
Análisis/Conclusión/Observación
Se pudo obtener información de los servicios habilitados, puertos de los servicios que utilizan, detalles del servidor, etc.
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces
ISSAF: • http://www.oissg.org/issaf.html SOFTWARE: • https://nmap.org/zenmap/
Herramientas
• Zenmap v7.6
Observaciones
• **Subfase de Metodología ISSAF:** Auditoria. • **Modo de Ataque:** Activo.

Fuente: Autoría Propia

Tabla 14: Prueba de Análisis de Configuración de Dispositivos

Prueba 7. Análisis de configuración de dispositivos
Objetivos
Verificar la configuración de los dispositivos de comunicación de la red inalámbrica.
Pre-requisitos
• Revisar Controles OWISAM.
Ejemplos/Resultados
Preguntas: 1) ¿Los dispositivos de comunicación inalámbrica son configurados por personal capacitado? Sí ___ No ___ 2) ¿Los dispositivos de comunicación cuentan con las últimas actualizaciones y parches de seguridad? Sí ___ No ___ 3) ¿Las credenciales de usuario y password de acceso a los dispositivos de comunicación están predeterminadas de fábrica? Sí ___ No ___

Resultados:



Análisis/Conclusión/Observación

Se concluye que los dispositivos de ambas sedes son configurados por personal capacitado, no se cuenta con las últimas actualizaciones y parches de seguridad en todos los dispositivos, y las credenciales de acceso a los dispositivos son predeterminadas de fábrica.

Contramedidas

Revisar el Plan de Mitigación de Riesgos.

Enlaces

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/
- https://auditoriawifi.es/controles-owisam/

Herramientas

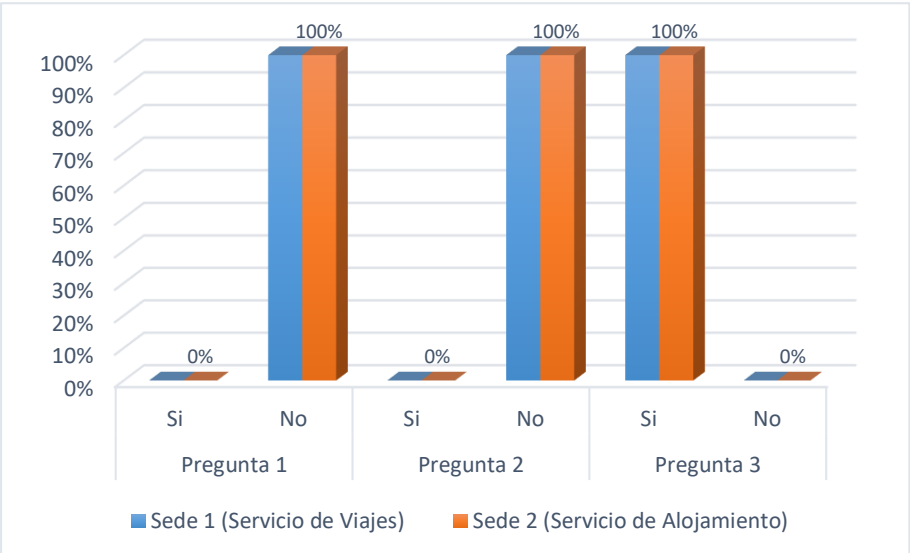
- Controles OWISAM.

Observaciones

- **Subfase de Metodología ISSAF:** Auditoria.
- **Control OWISAM:** Pruebas sobre directivas y normativa.
- **Subcontrol OWISAM:** Análisis de la configuración de dispositivos (OWISAM-GD-004).
- **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

Tabla 15: Prueba de Política de Gestión y Cambio de claves

Prueba 8. Análisis de la política de gestión y cambio de claves
Objetivos
Verificar la gestión de políticas para cambio de credenciales en la red inalámbrica de la Institución.
Pre-requisitos
• Revisar Controles OWISAM.
Ejemplos/Resultados
Preguntas: 1) ¿Los dispositivos de comunicación cuentan con contraseñas robustas? Sí ___ No ___ 2) ¿Las contraseñas de los dispositivos son cambiadas periódicamente? Sí ___ No ___ 3) ¿Existe personal autorizado para realizar cambio de contraseñas en los dispositivos de comunicación? Sí ___ No ___ **Resultados:**   
Análisis/Conclusión/Observación
Se concluye que ningún dispositivo de comunicación inalámbrica cuenta con contraseñas robustas, las contraseñas no son cambiadas periódicamente, y existe personal autorizado para realizar el cambio de contraseñas.

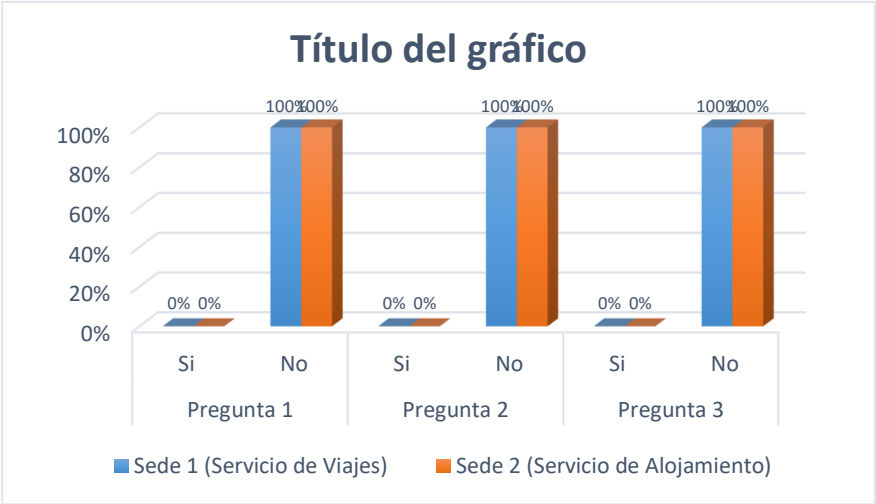
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces
OWISAM: • https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx • https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/ • https://auditoriawifi.es/controles-owisam/
Herramientas
• Metodología ISSAF. • Controles OWISAM.
Observaciones
• **Subfase de Metodología ISSAF:** Auditoria. • **Control OWISAM:** Pruebas sobre directivas y normativa. • **Subcontrol OWISAM:** Análisis de la política de gestión y cambio de claves (OWISAM-GD-005). • **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

Tabla 16: Prueba de Verificación de Inventario de Dispositivos

Prueba 9. Verificación de inventario de dispositivos autorizados
Objetivos
Verificar si el inventario de los dispositivos autorizados en la red está actualizado.
Pre-requisitos
• Revisar Controles OWISAM.
Ejemplos/Resultados
Preguntas: 1) ¿La Institución cuenta con un inventario de los dispositivos de comunicación inalámbrica? Sí ___ No ___ 2) ¿El inventario de los dispositivos es actualizado periódicamente? Sí ___ No ___ 3) ¿Existen políticas para el cambio o actualización de los dispositivos activos en la red? Sí ___ No ___

Resultados:



Análisis/Conclusión/Observación

Se concluye que la Institución en sus dos sedes no cuenta con un inventario actualizado de dispositivos de comunicación. Tampoco existen políticas para cambio o actualización de dispositivos.

Contramedidas

Revisar el Plan de Mitigación de Riesgos.

Enlaces

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/
- https://auditoriawifi.es/controles-owisam/

Herramientas

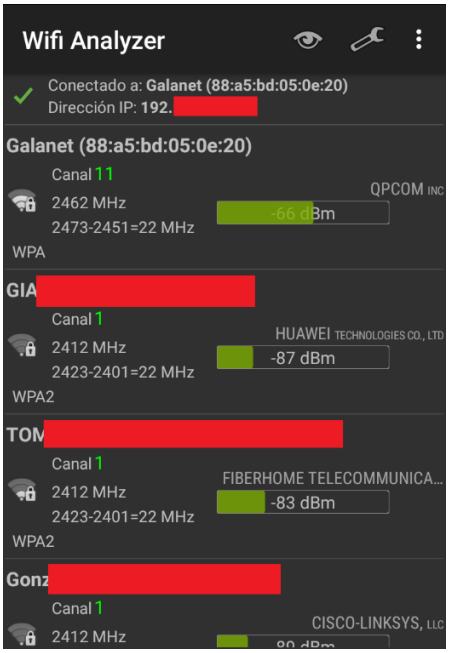
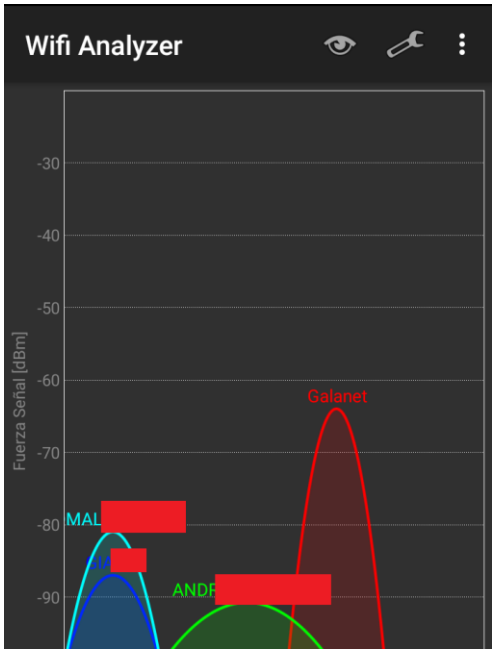
- Metodología ISSAF.
- Controles OWISAM.

Observaciones

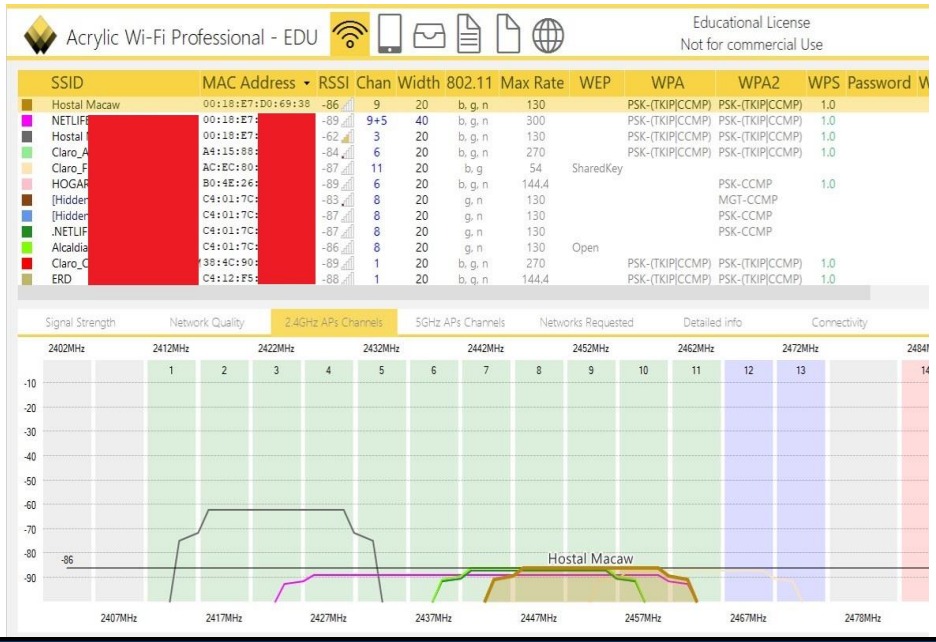
- **Subfase de Metodología ISSAF:** Auditoria.
- **Control OWISAM:** Pruebas sobre directivas y normativa.
- **Subcontrol OWISAM:** Verificación de inventario de dispositivos autorizados (OWISAM-GD-006).
- **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

Tabla 17: Prueba de Verificación del Nivel de Intensidad de Señal

Prueba 10. Verificación del nivel de intensidad de señal o área de cobertura
Objetivos
Verificar el área de cobertura de la red y el nivel de intensidad de la señal en la Institución.
Pre-requisitos
• Instalar Wifi Analyzer. • Instalar Acrylic Wifi Professional.
Ejemplos/Resultados
SEDE #1 - Servicio de Viajes    

SEDE #2 - Servicio de Alojamiento



Análisis/Conclusión/Observación

Se pudo verificar el nivel de la señal en ambas sedes; existen redes inalámbricas vecinas configuradas y que trabajan en el mismo área de cobertura de señal.

Contramedidas

Revisar el Plan de Mitigación de Riesgos.

Enlaces

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/
- https://auditoriawifi.es/controles-owisam/

SOFTWARE:

- https://www.acrylicwifi.com/

Herramientas

- Instalar Wifi Analyzer v3.11
- Instalar Acrylic Wifi Professional - EDU v3.2

Observaciones

- **Subfase de Metodología ISSAF:** Análisis y Búsqueda.
- **Control OWISAM:** Pruebas de configuración de la plataforma.
- **Subcontrol OWISAM:** Verificación del nivel de intensidad de señal o área de cobertura (OWISAM-CF-003).
- **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

Tabla 18: Prueba de Debilidades en el Firmware de AP

Prueba 11. Debilidades en el firmware de AP

Objetivos

Verificar si el firmware de los dispositivos de comunicación de la red está actualizado.

Pre-requisitos

- Revisar Controles OWISAM.

Ejemplos/Resultados

Ejemplos/Resultados:

- **Sede 1 (Servicio de Viajes)**

Equipo	Marca	Modelo	Firmware	Actualizado
Router	QPCOM	WR115N	v5.07	Si

- **Sede 2 (Servicio de Alojamiento)**

Equipo	Marca	Modelo	Firmware	Actualizado
Router	D-Link	DIR-635	v2.32	No

Análisis/Conclusión/Observación

Se constató que en la sede 1, no existe actualización de Firmware.

Contramedidas

Revisar el Plan de Mitigación de Riesgos.

Enlaces

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/
- https://auditoriawifi.es/controles-owisam/

Herramientas

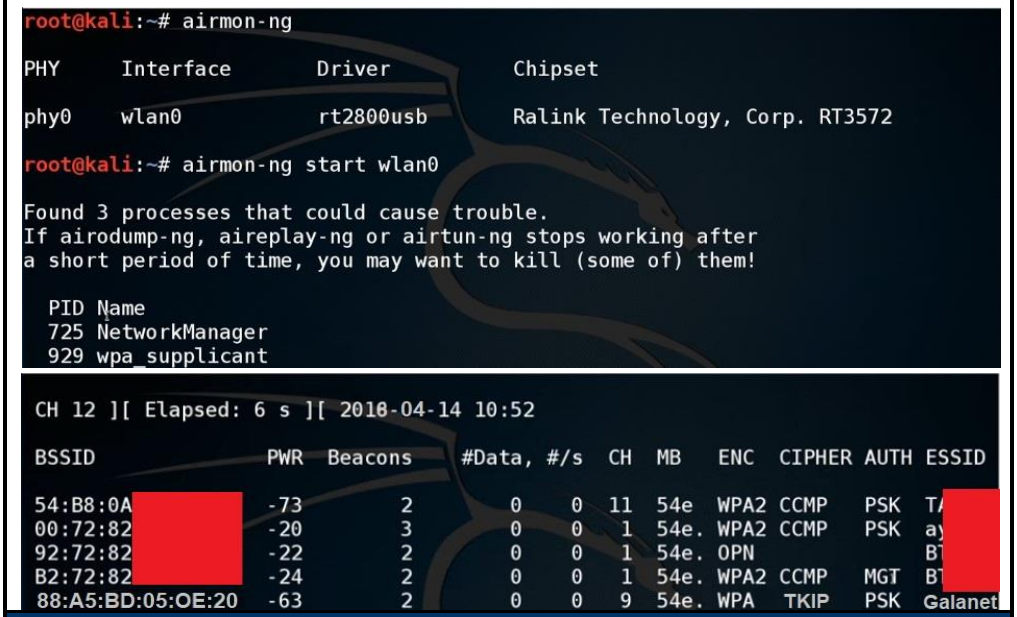
- Controles OWISAM.

Observaciones

- **Subfase de Metodología ISSAF:** Análisis y Búsqueda.
- **Control OWISAM:** Análisis de Infraestructura.
- **Subcontrol OWISAM:** Debilidades en el firmware del AP (OWISAM-IF-001).
- **Modo de Ataque:** Pasivo.

Fuente: Autoría Propia

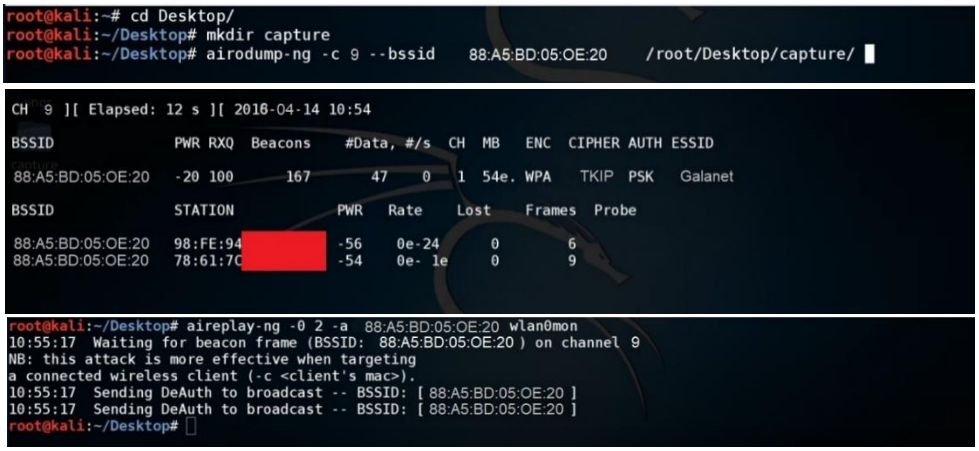
Tabla 19: Prueba de Análisis de Protocolos de Cifrado (WEP, TKIP)

Prueba 12. Análisis de protocolos de cifrado inseguro (WEP, TKIP..)
Objetivos
Analizar protocolos de cifrado (WEP, TKIP) y verificar la debilidad de seguridad en la red.
Pre-requisitos
• Instalar el Sistema Operativo Kali Linux, utilizar la suite Aircrack.
.Ejemplos/Resultados
SEDE #1 - Servicio de Viajes 
Análisis/Conclusión/Observación
Se identificó que en la Sede 1, los dispositivos inalámbricos están configurados con WPA PSK-TKIP, mientras que la Sede 2, tiene WPA2 PSK-(TKIP-CCMP).
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces
OWISAM: • https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx • https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/ SOFTWARE: • https://www.kali.org/
Herramientas
• Kali Linux 64bits 2017

Observaciones
• **Subfase de Metodología ISSAF:** Análisis y Búsqueda. • **Control OWISAM:** Pruebas de cifrado de comunicaciones. • **Subcontrol OWISAM:** Análisis de protocolos de cifrado inseguro (WEP, TKIP) (OWISAM-CP-004). • **Modo de Ataque:** Activo.

Fuente: Autoría Propia

Tabla 20: Prueba de Captura y Cracking de Claves Transmitidas

Prueba 13. Captura y cracking de claves transmitidas en el proceso de autenticación
Objetivos
Verificar la captura de las contraseñas que son transmitidas durante la autenticación a la red wifi.
Pre-requisitos
• Instalar el Sistema Operativo Kali Linux, utilizar la suite Aircrack.
Ejemplos/Resultados
SEDE #1 - Servicio de Viajes 
Análisis/Conclusión/Observación
En la Sede 1 no se pudieron obtener las contraseñas con cifrado WPA; mientras en la Sede 2 se pudo forzar la conexión debido que se tiene habilitado WPS.
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces

OWISAM:

- https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx
- https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/
- https://auditoriawifi.es/controles-owisam/

SOFTWARE:

- https://www.kali.org/

Herramientas

- Kali Linux 64bits 2017

Observaciones

- **Subfase de Metodología ISSAF:** Explotación y Ataque.
- **Control OWISAM:** Pruebas sobre la autenticación.
- **Subcontrol OWISAM:** Captura y cracking de claves transmitidas en el proceso de autenticación (OWISAM-AU-004).
- **Modo de Ataque:** Activo.

Fuente: Autoría Propia

Tabla 21: Pruebas de Deautenticación

Prueba 14. Pruebas de deautenticación

Objetivos

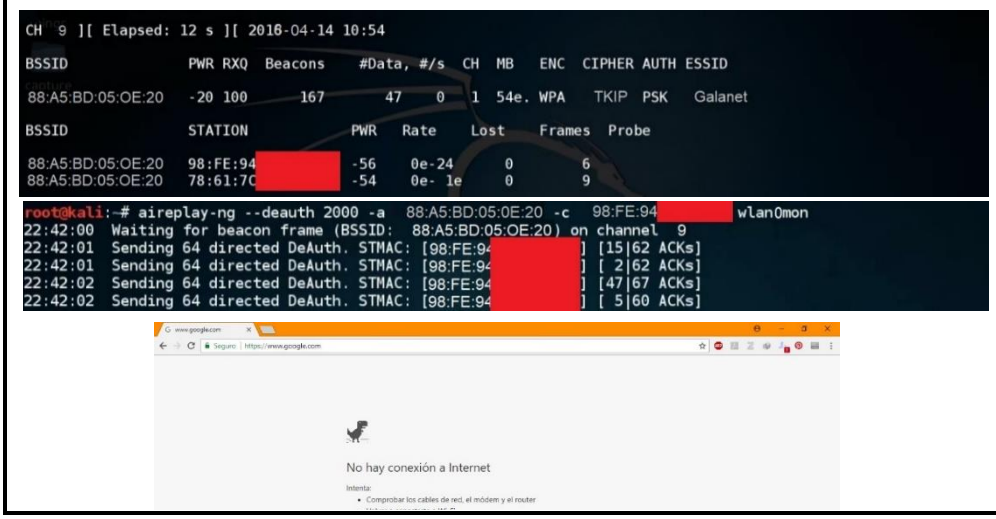
Desconectar a los usuarios, impidiendo el uso de servicios en la red inalámbrica.

Pre-requisitos

- Instalar el Sistema Operativo Kali Linux, utilizar la suite Aircrack.

Ejemplos/Resultados

SEDE #1 - Servicio de Viajes



Análisis/Conclusión/Observación
Se realizó deautenticación del servicio de Internet a un usuario como ejemplo, obligándolo a conectarse nuevamente a la red.
Contramedidas
Revisar el Plan de Mitigación de Riesgos.
Enlaces
OWISAM: • https://www.owisam.org/es/Archivo:Controles_OWISAM_ES.xlsx • https://www.tarlogic.com/servicios/auditoria-wireless-seguridad-wifi-owisam/ • https://auditoriawifi.es/controles-owisam/ SOFTWARE: • https://www.kali.org/
Herramientas
• Kali Linux 64bits 2017
Observaciones
• **Subfase de Metodología ISSAF:** Explotación y Ataque. • **Control OWISAM:** Denegación de servicio. • **Subcontrol OWISAM:** Pruebas de deautenticación (OWISAM-DS-001). • **Modo de Ataque:** Activo.

Fuente: Autoría Propia

4.5. Identificación del Activo Crítico

El activo critico representa el recurso más importante dentro de una Institución, y su identificación permite conocer cuáles deben ser resguardados con mayor control. El activo crítico de este proyecto se centra en la red inalámbrica. Dicha red en sus 2 Sedes presenta varias características:

- **Tipo de red Inalámbrica (IEEE):** Sede Servicio de Viajes (802.11 b, g) y Sede servicio de Alojamiento (802.11 b, g, n).

- **Mecanismo de autenticación:** WPA y WPA2.
- **Tipo de encriptación:** PSK-TKIP y PSK-(TKIP│CCMP)
- **Longitud de clave Wifi:** 10 dígitos, en ambas sedes.
- **Gateway configurado por defecto:** Si, en ambas sedes.
- **Contraseñas de dispositivos inalámbricos por defecto:** Si, en la Sede de Alojamiento.
- **WPS habilitado:** Si, en la Sede de Alojamiento.
- **SSID configurado por defecto:** No, en ambas sedes.

4.6. Identificación de Vulnerabilidades en la Red Wifi

Las vulnerabilidades son debilidades del sistema informático, utilizadas para ocasionar daños tanto en el hardware como en el software. Las vulnerabilidades encontradas según la ejecución de las pruebas de seguridad se detallan en la Tabla 22.

Tabla 22: Vulnerabilidades en la Red Wifi

SubFase ISSAF	Pruebas/Controles OWISAM	Vulnerabilidades
Recopilación Información	Descubrimiento activo de dispositivos y redes.	• Descubrimiento de información de la red wifi.

Escaneo	Identificación de funcionalidades soportadas por el dispositivo.	• Conseguir información sobre los dispositivos de comunicación inalámbrica (software y hardware).
Auditoría	Pruebas sobre WPS.	• Acceso no autorizado a redes Wifi. • Mecanismo de autenticación WPS habilitado.
	Interfaces administrativas expuestas a la red.	• Acceso no autorizado e intercepción de tráfico. • Acceso a la administración de dispositivos a través del Gateway predeterminado.
	Prueba de Traceroute	• Direcciones IPs evidentes al mapear los saltos de la red.
	Prueba de AP/Router	• Obtención de puertos, servicios y protocolos habilitados.
	Análisis de configuración de dispositivos.	• Configuración de dispositivos incorrecta. • Falta de políticas de configuración de dispositivos.
	Análisis de la política de gestión y cambio de claves.	• Período elevado de duración de contraseñas. • Falta de políticas de gestión y cambio de claves.
	Verificación de inventario de dispositivos autorizados.	• Falta de inventario de dispositivos actualizado.
Análisis y Búsqueda	Verificación del nivel de intensidad de señal o área de cobertura.	• Area de cobertura excesiva. • Emisión de señal de clientes no autorizados.
	Debilidades en el firmware del AP.	• Robo de credenciales y acceso no autorizado. • Falta de actualización de Firmware del Router.

	Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)	• Seguridad de red inalámbrica débil. • Intercepción de comunicación. • Obtención de información sensible.
Explotación y Ataque	Captura y cracking de claves transmitidas en el proceso de autenticación.	• Claves débiles.
	Pruebas de deautenticación.	• Intercepción de credenciales de autenticación.

Fuente: Autoría Propia

4.7. Análisis de Riesgos

El análisis de riesgos pretende evaluar los peligros potenciales y las consecuencias dentro del desarrollo del proyecto; con el fin de establecer medidas de prevención y protección para los activos de la información. Durante esta etapa seguiremos los lineamientos que nos brinda la metodología Magerit para evaluar riesgos.

4.7.1. Análisis de Impacto

El impacto es el daño causado por la ocurrencia de una contingencia. Existen varios criterios para estimar el impacto, a través de una escala del 1 al 5. Los criterios para estimar el impacto se muestran en la Tabla 23.

Tabla 23: Criterios para Estimar el Impacto

Impacto	Valor	Descripción
Muy Bajo	**1**	El daño derivado de la materialización de la amenaza, no tiene consecuencias relevantes para la Institución.
Bajo	**2**	El daño derivado de la materialización de la amenaza, tiene consecuencias leves para la Institución.
Medio	**3**	El daño derivado de la materialización de la amenaza, tiene consecuencias destacables para la Institución.
Alto	**4**	El daño derivado de la materialización de la amenaza, tiene consecuencias graves para la Institución.
Muy Alto	**5**	El daño derivado de la materialización de la amenaza, tiene consecuencias muy graves para la Institución.

Fuente: Autoría Propia

4.7.2. Estimación de Riesgo

Un riesgo es un suceso que se presenta en un sitio concreto durante un intervalo de tiempo. Para la estimación del riesgo es conveniente utilizar la *Matriz de Probabilidad-Impacto,* que es una herramienta de análisis cualitativo y permite categorizar los riesgos en varios niveles de importancia. La Tabla 24, muestra los niveles de riesgos utilizados durante el proyecto.

Tabla 24: Niveles de Estimación de Riesgos

Nivel de Riesgo	Valor	Impacto
Riesgo Marginal	**1 - 2**	Mantener vigilancia, aunque no requiere medidas preventivas.
Riesgo Apreciable	**3 - 8**	Analizar introducir económicamente medidas preventivas, para reducir el nivel de riesgo.
Riesgo Importante	**9 - 12**	Medidas preventivas obligatorias. Controlar fuertemente las variables de riesgo durante el proyecto.
Riesgo Muy Grave	**15 - 25**	Requiere medidas preventivas urgentes.

Fuente: Autoría Propia

La Tabla 25, muestra la matriz de riesgos que está compuesta por columnas (valores promedio de probabilidad) y filas (valores promedio de impacto del riesgo).

Tabla 25: Matriz de Riesgos

		PROBABILIDAD				
		Muy Baja 1	Baja 2	Media 3	Alta 4	Muy Alta 5
IMPACTO	Muy Alto 5	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Medio 3	3	6	9	12	15
	Bajo 2	2	4	6	8	12
	Muy Bajo 1	1	2	3	4	5

Fuente: Autoría Propia

Para obtener el riesgo equivalente se multiplica el nivel de probabilidad (np) de la ocurrencia de una amenaza, por la gravedad o nivel del impacto (ni) del daño. La fórmula del riesgo equivalente se presenta en la Figura 4.1.

$$Nivel\ de\ Riesgo = (np * ni)$$

Figura 4.1: Fórmula del Nivel de Riesgo

Fuente: Autoría Propia

4.7.3. Evaluación de Riesgo y Mapa de Calor

Para elaborar esta etapa fue necesario previamente haber identificado el activo crítico, que para este proyecto es la red inalámbrica de la Institución. Posteriormente se realizó la recolección de la información a través de entrevistas, pruebas de seguridad, observación, documentación etc., y se identificaron las vulnerabilidades y amenazas existentes.

En la Tabla 26, se presenta la Matriz de Probabilidad-Impacto, que contiene el valor del riesgo encontrado por cada amenaza y vulnerabilidad en la red Wifi. Los niveles de riesgo sobre el cual se elaborará el plan de mitigación serán: riesgo apreciable, riesgo importante y riesgo muy grave.

Tabla 26: Matriz de Evaluación de Riesgos

No	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Valor de Riesgo	Nivel de Riesgo
1	Acceso No autorizado	Acceso No autorizado a redes Wifi.	4	4	16	Muy Grave
2	Daños por agua	Lluvias, rotura de tuberías	3	4	12	Importante
3	Escuchas encubiertas	Emisión de señal de clientes no autorizados.	5	3	15	Muy Grave
4	Espionaje	Ataques de disponibilidad del servicio.	3	4	12	Importante
5		Descubrimiento de información de la red Wifi.	3	3	9	Importante
6		Intercepción de la comunicación.	4	4	16	Muy Grave
7		Obtención de información sobre hardware y software.	3	3	9	Importante
8		Obtención de puertos, servicios y protocolos habilitados.	3	3	9	Importante
9	Falla de políticas de seguridad inalámbrica	Configuración de dispositivos incorrecta.	4	4	16	Muy Grave
10		Claves o Credenciales débiles.	4	4	16	Muy Grave
11		Falta de políticas de configuración de dispositivos.	5	5	25	Muy Grave
12		Falta de políticas de gestión y cambio de claves	5	5	25	Muy Grave
13		Falta de políticas de uso y restricción de la red Wifi.	5	5	25	Muy Grave
14		Falta de inventario de dispositivos actualizado.	5	5	25	Muy Grave

15		Tiempo de vida de contraseñas elevado.	5	5	25	Muy Grave
16	Falla en la seguridad de la comunicación	Obtención de información sensible.	4	5	20	Muy Grave
17	Fraude	Engaño o estafa.	3	4	12	Importante
18	Fuego	Falta de políticas de acción contra fuego.	3	4	12	Importante
19	Incorrecta configuración de la red inalámbrica	Acceso a recursos de la red.	4	3	12	Importante
20		Acceso a la administración de dispositivos usando Gateway predeterminado.	4	3	12	Importante
21		Área de cobertura excesiva.	4	3	12	Importante
22		Direcciones IPs evidentes al mapear saltos de red.	4	3	12	Importante
23		Mecanismo de autenticación WPS habilitado.	4	4	16	Muy Grave
24	Incorrecto mantenimiento de la red inalámbrica	Inadecuado control en los mantenimientos de la red.	4	4	16	Muy Grave
25		Susceptibilidad del equipamiento a la humedad y contaminación.	4	4	16	Muy Grave
26	Ingeniería social	Acceso No autorizado e intercepción de tráfico.	5	5	25	Muy Grave
27	Intercepción de información	Intercepción de credenciales de autenticación.	4	5	20	Muy Grave
28	Robo común	Acceso a las instalaciones y	5	5	25	Muy Grave

		equipos inalámbricos.				
29	Virus	Daño de la información.	2	3	6	Apreciable
Promedio					**471**	

Fuente: Autoría Propia

Mapa de Calor de Riesgos:

En la Figura 4.2, se representan los datos sobre el mapa de calor, donde se agrupan los riesgos según el grado de criticidad.

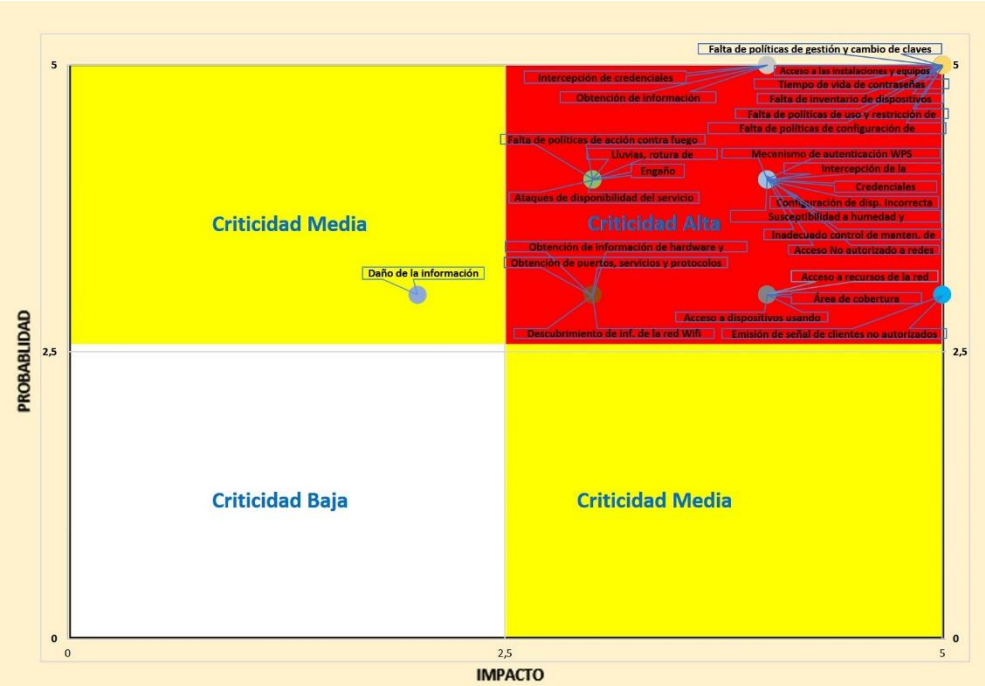


Figura 4.2: Mapa de Calor de Riesgos

Fuente: Autoría Propia

Los niveles de riesgo obtenidos en porcentajes, indicando su grado de criticidad se presentan en el **Anexo # 5.**

4.8. Tratamiento del riesgo

El tratamiento del riesgo constituye un proceso de selección e implementación de medidas de seguridad que permiten mitigar el riesgo, brindando la solución más óptima a la red de la Institución en el menor tiempo y con el menor costo posible.

Luego del análisis de riesgos realizado sobre la red inalámbrica, se deberá elaborar un plan de mitigación de riesgos; que contiene recomendaciones basadas en el estándar ISO/IEC 27002:2013, y la metodología OWISAM sobre cada una de las vulnerabilidades encontradas.

Cabe destacar que el tratamiento se aplicará sobre aquellas vulnerabilidades que tienen un nivel de riesgo: muy grave, importante, y apreciable.

CAPÍTULO 5

PLAN DE MITIGACIÓN DE RIESGOS

En este Capítulo se desarrolla el plan de mitigación de riesgos y el análisis de factibilidad que incluye un análisis de factibilidad técnico, operativo y económico.

5.1. Plan de Mitigación

Con los cambios tecnológicos en las redes de comunicaciones; surge la necesidad de implementar mecanismos, estándares y directrices que garanticen la seguridad de las redes inalámbricas.

Luego de la evaluación de riesgo; es indispensable la elaboración de un plan de mitigación de riesgos, basado en estándares ISO/IEC 27002:2013 y la metodología OWISAM. Éste plan contendrá estrategias definidas por el administrador de red, para reducir la probabilidad de ocurrencia o el impacto que pueda ocasionar un riesgo en la red inalámbrica de la Institución.

5.1.1. Alcance del Plan

El plan de mitigación de riesgos comprende la seguridad de la red inalámbrica de la Institución, a través de recomendaciones que definen las acciones más optimas a seguir.

5.1.2. Objetivo del Plan

“Definir recomendaciones, directrices y normas que permitan reducir los riesgos manteniendo la disponibilidad del servicio de la red inalámbrica”.

5.1.3. Responsabilidades

La responsabilidad recae sobre el administrador de red; mismo que deberá someter a revisión los procedimientos establecidos en el Plan.

5.1.4. Evaluación de Daños

El administrador de red tendrá la responsabilidad de identificar el activo crítico que para este proyecto es la red inalámbrica; evaluar las amenazas y vulnerabilidades en la fase de análisis de riesgos y posteriormente documentar la evaluación final de los daños y las acciones efectuadas.

5.1.5. Pruebas del Plan y Capacitaciones

Se recomienda realizar pruebas del plan de mitigación y capacitaciones cada 6 meses, para garantizar su correcta funcionalidad.

5.1.6. Actualización del Plan

El administrador de red tiene la responsabilidad de mantener actualizado el plan de mitigación, y comunicar al Representante Legal de la Institución los cambios en las nuevas versiones. Se recomienda actualizar el Plan al menos una vez al año.

5.1.7. Elaboración del Plan

La Tabla 27, contiene el plan de migración de riesgos .

Tabla 27: Plan de Mitigación de Riesgos

No	Amenaza	Vulnerabilidad	Valor/ Nivel de Riesgo	Controles o Recomendaciones Norma ISO/IEC 27002:2013 y Metodología OWISAM
1	Acceso No autorizado	Acceso No autorizado a redes Wifi.	16/ Muy Grave	• Cambiar los parámetros de configuración predeterminada en los dispositivos inalámbricos. • Establecer el tipo de cifrado WPA2 con el algoritmo de encriptación AES CCMP. • Cambiar las contraseñas de seguridad inalámbrica cada 6 meses, usando al menos 12 caracteres alfanuméricos. • Cambiar la contraseña de administración y limitar el acceso a la administración del Router Wifi desde otras redes como Internet. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa.
2	Daños por agua	Lluvias, rotura de tuberías	12/ Importante	• Realizar Mantenimiento preventivo 1 vez por año al sistema de agua potable. • Disponer de los Planos de distribución del sistema de agua potable. • Identificar lugares susceptibles a inundaciones y gestionar las medidas de seguridad necesarias. • Ubicar los equipos de comunicación inalámbrica en lugares estratégicos, fuera de lugares propensos a roturas de tuberías. • Disponer de equipos de comunicación alternos para reanudar los servicios de comunicación. • Verificar que las instalaciones eléctricas estén en correcto estado de funcionamiento para evitar cortocircuitos.
3	Escuchas encubiertas	Emisión de señal de clientes no autorizados.	15/ Muy Grave	• Establecer el tipo de cifrado WPA2 con el algoritmo de encriptación AES CCMP.

				• Actualizar el firmware del dispositivo a la última versión, con todos los parches de seguridad. • Cambiar las contraseñas de seguridad inalámbrica cada 6 meses, usando al menos 12 caracteres. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa. • Medir la propagación de la señal Wifi y ajustar los parámetros del punto de acceso, con el fin de evitar una propagación no deseada de la red. • Seleccionar la óptima ubicación de los dispositivos inalámbricos, para mejorar el rendimiento Wifi.
4	Espionaje	Ataques de disponibilidad del servicio.	12/ Importante	• Establecer el tipo de cifrado WPA2 con el algoritmo de encriptación AES CCMP. • Actualizar el firmware del dispositivo a la última versión, con todos los parches de seguridad. • Deshabilitar los beacon frame en los dispositivos de comunicación inalámbrica. • Habilitar la opción logging (log), que permite llevar un control de las conexiones del Router. • Realizar un monitoreo de las conexiones TCP/UDP en la red de la Institución. • Resguardar físicamente los equipos de comunicación inalámbrica del público y empleados, evitando su uso indebido. • Deshabilitar la funcionalidad de compatibilidad del AP con redes 802.11b permitiendo únicamente conexiones Wifi que sigan el estándar 802.11g, en caso de que no sea imprescindible.

5		Descubrimiento de información de la red Wifi.	9/ Importante	• Deshabilitar los beacon frame en los dispositivos de comunicación inalámbrica. • Eliminar las redes favoritas (hoteles, cafeterías...) que no se van a volver a utilizar de los dispositivos. • Si se define una red oculta, evaluar que existen controles de seguridad compensatorios. • Verificar que no se tenga configurada la opción de “conexión automática” por parte de los clientes que acceden a las redes wifi, aunque la red no se encuentre emitiendo. • Disponer de políticas claras, conocidas por todo el personal sobre el uso de dispositivos con capacidades Wifi. • Mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de Rogue APs. • Evitar el uso de nombres genéricos en las redes de comunicaciones Wifi; que no identifiquen a la organización, e impidan ataques de suplantación de identidad de los puntos de acceso. • Disponer de un sistema de detección de intrusos WIDS (Wireless Intrusion Detection System), que detecte y comunique la aparición de nuevos dispositivos o comportamientos extraños.
6		Intercepción de la comunicación.	16/ Muy Grave	• Limitar el acceso a conexiones de las interfaces administrativas, sólo a través de la red cableada o únicamente a una serie de IPs reservadas. • Verificar que no se tenga configurada la opción de “conexión automática” por

				parte de los clientes que acceden a las redes wifi, aunque la red no se encuentre emitiendo. • Establecer el tipo de cifrado WPA2 con el algoritmo de encriptación AES CCMP. • Actualizar el firmware del dispositivo a la última versión, con todos los parches de seguridad. • Cambiar las contraseñas de las interfaces administrativas por defecto para su acceso, por otras más robustas cada mes. • Mantener un log de eventos de todo lo que ocurre en el AP para detectar cualquier intrusión o intento de explotar una vulnerabilidad.
7		Obtención de información sobre hardware y software.	9/ Importante	• Monitorizar periódicamente la actividad en busca de nuevos puntos de acceso que puedan haber sido desplegados con el objetivo de robar credenciales de acceso o atacar a los clientes. • Monitorización de tráfico y logs con alguna herramienta como Wireshark o kismet en busca de comportamientos anómalos. • Deshabilitar los beacon frame en los dispositivos de comunicación inalámbrica.
8		Obtención de puertos, servicios y protocolos habilitados.	9/ Importante	• Eliminar los métodos de autenticación inseguros y permitir únicamente aquel que se vaya a utilizar. • Configurar los servicios en puertos no habituales. • Anular información del protocolo que informe sobre el tipo de servicio, evitando firmas que indican las versiones y mensajes de bienvenida. • Configurar un firewall apropiado, para que los servicios solo estén

				disponibles desde IPs autorizadas • Limitar el acceso a conexiones de las interfaces administrativas, sólo a través de la red cableada o únicamente a una serie de IPs reservadas. • Realizar un examen de los puertos de red inseguros basado en las aplicaciones, vulnerabilidades y ataques asociados, con el fin de brindar enfoques de protección. • Mantener un inventario de todos los dispositivos autorizados, o al menos de los puntos de acceso, para facilitar la detección de Rogue APs. • Instalar solo lo necesario, para evitar tener demasiados servicios accesibles desde fuera de la red.
9	Falla de políticas de seguridad inalámbrica	Configuración de dispositivos incorrecta.	16/ Muy Grave	• Capacitar al administrador de la red sobre el uso y configuración de los dispositivos de comunicación actuales y nuevos. • Elaborar un manual de corrección de errores de la red, a fin de documentar las incidencias y las soluciones brindadas. • Evitar el acceso físico de personal No autorizado sobre los dispositivos de comunicación. • Controlar el tiempo de uso de los dispositivos de comunicación. • Determinar la ubicación más óptima de los dispositivos de comunicación Wifi. • Realizar mantenimientos preventivos de la red cada 3 meses. • Llevar un inventario actualizado de los dispositivos de comunicación.

10		Credenciales débiles.	16/ Muy Grave	• Usar mecanismos de autenticación robustos, como WPA2-CCMP. • Evitar credenciales genéricas o predecibles y habilitar la renovación automática de claves de ser el caso. • Cambiar las contraseñas de las interfaces administrativas por defecto para su acceso, y actualizarlas 1 vez cada mes. • Usar contraseñas robustas (12 caracteres mínimo, incluyendo letras mayúsculas, números y símbolos especiales). • Disponer de políticas de contraseñas, para dificultar los ataques basados en diccionario. • Disponer de algún sistema de protección ante ataques de fuerza bruta. • Evaluar si es posible por implantar una solución RADIUS. • Almacenar en forma de hashes las credenciales de acceso de cada usuario, usando un algoritmo criptográfico seguro (SHA-2), cifrados con una clave única y robusta definida por el administrador. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa.
11		Falta de políticas de configuración de dispositivos.	25/ Muy Grave	• Elaborar un manual de políticas de configuración de dispositivos, mantenerlo actualizado y controlar que se cumpla. • Capacitar al administrador de la red sobre el uso y configuración de los dispositivos de comunicación actuales y nuevos. • Llevar un inventario actualizado de los dispositivos de comunicación.

				• Usar dispositivos que cumplan el estándar, ya que son más fáciles de monitorizar y tener controlados. • Controlar el tiempo de uso de los dispositivos de comunicación.
12		Falta de políticas de gestión y cambio de claves	25/ Muy Grave	• Evitar emplear siempre la misma clave y rotarla, para asegurar que ninguna persona No autorizada tenga acceso a los recursos de la misma que se quieren proteger. • Elaborar políticas para contraseñas, que implanten una robustez mínima y una duración temporal máxima, mantenerlas actualizadas y controlar que se cumpla. • Verificar que los routers permiten definir un tiempo de vida máximo para las claves de cifrado dentro de la red Wifi, tras el cual se deberán generar nuevas. Esta funcionalidad debería estar activada y con un valor no superior a 3600s, para evitar ataques a la red Wifi. • Establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.
13		Falta de políticas de uso y restricción de la red Wifi.	25/ Muy Grave	• Evitar emplear las redes Wifi de la Institución para tareas críticas, debido a los riesgos que suponen. • Verificar qué dispositivos y usuarios están autorizados para emplear las redes Wifi y así poder mantener un control sobre las mismas. • Elaborar un manual de políticas de uso y restricción de la red Wifi, mantenerlo actualizado y controlar que se cumpla.

				• Usar mecanismos de autenticación robustos, como WPA2-CCMP. • Mantener aislada la red Wifi de acceso público, del resto de segmentos importantes de la red de la Institución. • Realizar un filtrado de dirección MAC; una dirección física de la tarjeta de red del dispositivo que podemos introducir en el Router para que sólo pueda acceder dicha dirección de red. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa. • Utilizar un portal cautivo, donde el usuario que quiera acceder tiene que aceptar explícitamente las condiciones de acceso a la red Wifi.
14		Falta de inventario de dispositivos actualizado.	25/ Muy Grave	• Elaborar un inventario de dispositivos autorizados, mantenerlo actualizado y controlar que se cumpla. • Realizar un análisis periódico de verificación de inventarios, que permitirá detectar accesos No autorizados y desviaciones en la normativa interna. • Analizar que los dispositivos identificados durante las pruebas de monitorización activa y pasiva se corresponden con los existentes en el inventario. • Identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información. • Verificar que toda la información y activos del inventario asociados a los recursos para el tratamiento de la información

				pertenezcan a una parte designada de la Institución.
15		Tiempo de vida de contraseñas elevado.	25/ Muy Grave	• Evitar emplear siempre la misma clave; es necesario ir rotando para asegurar que ninguna persona No autorizada, tiene acceso a los recursos de la misma que se quieren proteger. • Elaborar políticas para contraseñas, que implanten una robustez mínima y una duración temporal máxima, mantenerlas actualizadas y controlar que se cumpla. • Establecer políticas para que se realice un cambio de claves periódico en las redes Wifi que hacen uso de un secreto compartido (PSK). • Analizar el tráfico de red recopilado y comprobar si se produce algún intercambio de claves de forma regular.
16	Falla en la seguridad de la comunicación	Obtención de información sensible.	20/ Muy Grave	• Utilizar el sistema de cifrado más robusto en la actualidad (AES-CCMP) del que se dispone a nivel de capa de enlace Usar en las capas superiores soluciones de tipo VPN, IPSec o SSL. • Asegurar que esté desactivada la autenticación por clave compartida. • Evitar las redes abiertas dentro de la Institución, ya que crean nuevos segmentos de ataque que podría aprovechar un usuario malintencionado. • Analizar en tiempo real la información que está siendo transmitida a través de la red, empleando para ello algún sistema IDS flexible. • Cambiar la contraseña de la red Wifi por una clave nueva, que tenga al menos 12 caracteres (combine letras mayúsculas y minúsculas, símbolos y números).

				• Realizar un filtrado de dirección MAC; una dirección física de la tarjeta de red del dispositivo que podemos introducir en el Router para que sólo pueda acceder dicha dirección de red. • Mantener invisible las redes Wifi de la Institución, siendo necesario introducir su nombre exacto para poder conectarse.
17	Fraude	Engaño o estafa.	12/ Importante	• Utilizar el sistema de cifrado más robusto en la actualidad (AES-CCMP) del que se dispone a nivel de capa de enlace Usar en las capas superiores soluciones de tipo VPN, IPSec o SSL. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa. • Actualizar regularmente el sistema operativo y el software base instalado en el equipo. • Instalar un antivirus bajo licencia y mantenerlo actualizado. • Instalar un firewall con el fin de restringir accesos No autorizados desde Internet. • Utilizar contraseñas seguras compuestas por 12 caracteres (combine letras mayúsculas y minúsculas, símbolos y números). • Modificar las contraseñas de los dispositivos con frecuencia al menos 1 vez cada mes. • Evitar las redes abiertas dentro de la Institución, ya que generan nuevos vectores de ataque que un usuario maligno podría aprovechar. • Navegar por páginas web seguras y de confianza, que tengan algún sello o certificado garantizando su calidad y fiabilidad.

				• Mantener cuidado al utilizar programas de acceso remoto. • Poner especial atención en el uso del correo electrónico, evitando abrir mensajes desconocidos y compartir información. • Capacitar al personal de la Institución sobre la importancia de proteger la información. • Evitar la descarga e instalación de software poco confiable. • Contactar a una firma experta en seguridad de la información e investigaciones forenses que pueda analizar la información contenida en los activos de información de ser el caso. • Realizar un filtrado de dirección MAC. • Comprobar los equipos que se conectan a la red Wifi, para detectar la presencia de intrusos.
18	Fuego	Falta de políticas de acción contra fuego.	12/ Importante	• Mantener los extintores manuales debidamente cargados y en buen estado de funcionamiento. • Capacitar al personal sobre el correcto uso de extintores a través de personal especializado. • Realizar respaldos internos y externos de toda la información de los dispositivos de la Institución. • Realizar un mantenimiento periódico de las instalaciones eléctricas y verificar que estén en correcto estado de funcionamiento. • Identificar y señalar adecuadamente las rutas de evacuación. • Instalar detectores de humo en logares específicos de la Institución.

				• Mantener los activos de información conectados a un sistema de tierras. • Mantener limpio y en orden el área de trabajo, evitando la acumulación de sustancias y productos inflamables. • Verificar que los niveles de voltaje sean los adecuados para los equipos informáticos. • Disponer de los Planos eléctricos de la Institución. • Realizar simulacros contra incendios cada 6 meses. • Localizar los números telefónicos de emergencia (cuerpo de bomberos, ambulancias y personal de la Institución responsable de las acciones de contingencia). • Adquirir un seguro contra incendios de ser el caso.
19	Incorrecta configuración de la red inalámbrica	Acceso a recursos de la red.	12/ Importante	• Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa. • Desactivar la difusión de la red Wifi. • Usar el sistema de cifrado más robusto actualmente (AES-CCMP) del que se dispone a nivel de capa de enlace. • Desactivar la opción “Mostrar Caracteres” para impedir visualizar la contraseña de la red Wifi del dispositivo conectado. • Cambiar la contraseña de la red Wifi por una clave nueva, que tenga al menos 12 caracteres (combine letras mayúsculas y minúsculas, símbolos y números). • Realizar un filtrado de dirección MAC. • Verificar los equipos que se conectan a la red Wifi, para detectar la presencia de intrusos. • Realizar mantenimiento a las cámaras de seguridad y

				cambiar las credenciales de administración 1 vez cada mes. • Cambiar la contraseña de administración del Router.
20		Acceso a la administración de dispositivos usando Gateway predeterminado.	12/ Importante	• Cambiar la puerta de enlace (Gateway) predeterminado en los dispositivos de comunicación inalámbrica. • Limitar el acceso a conexiones de las interfaces administrativas, sólo a través de la red cableada o únicamente a una serie de IPs reservadas. • Deshabilitar las propiedades de intercambio por internet y detección de redes en los equipos. • Cambiar las contraseñas de las interfaces administrativas por defecto para su acceso, por otras más robustas cada mes.
21		Área de cobertura excesiva.	12/ Importante	• Realizar un análisis de cobertura o Site Survey Wifi tanto en el interior como en el exterior de la Institución, mapeando los niveles de señal de las redes con el objetivo de identificar aquellos puntos de acceso con niveles de señal altos. • Controlar y limitar la potencia con la que los APs difunden la red, evitando que el perímetro de cobertura exceda más de lo imprescindible fuera de los límites de la Institución. • Limitar el alcance de los puestos de trabajo con interfaz Wifi, evitando que se pueda establecer comunicaciones con ellos desde el exterior. • Evitar que los enlaces Wifi sean accesibles a mayor distancia de la esperada, revisando los parámetros Slottime, ACK y CTS Timeout.

				• Las redes Wifi de la Institución deberían estar configuradas en diferentes canales sin solapamiento. Siempre que las limitaciones del hardware lo permitan y no se requiera un gran rango de cobertura, es aconsejable usar la banda de frecuencias de 5GHz, ya que los canales tienen un menor solapamiento debido al mayor ancho de banda a costa de perder alcance efectivo. • Se recomienda utilizar el canal 1, 6 u 11, siendo menos propensos a la saturación por su relación con el resto de canales.
22		Direcciones IPs evidentes al mapear saltos de red.	12/ Importante	• Limitar el acceso a conexiones de las interfaces administrativas, sólo a través de la red cableada o únicamente a una serie de IPs reservadas. • Modificar las contraseñas de los dispositivos con frecuencia al menos 1 vez cada mes. • Cambiar la contraseña de la red Wifi por una clave nueva, que tenga al menos 12 caracteres (combine letras mayúsculas y minúsculas, símbolos y números). • Realizar un filtrado de dirección MAC. • Verificar los equipos que se conectan a la red Wifi, para detectar la presencia de intrusos.
23		Mecanismo de autenticación WPS habilitado.	16/ Muy Grave	• Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa. • Cambiar los parámetros de configuración predeterminada en los dispositivos inalámbricos. • Establecer el tipo de cifrado WPA2 con el algoritmo de encriptación AES CCMP.

				• Realizar el cambio de la clave de fábrica de cualquier Router Wifi para evitar la exposición de ataques. • Verificar la configuración del servidor de autenticación RADIUS y de los mecanismos de autenticación soportados de ser el caso. Es necesario eliminar los métodos de autenticación inseguros y permitir únicamente aquel que se vaya a utilizar. • Evitar el uso de la dirección MAC de la interfaz Wifi del dispositivo (o un valor derivado) así como el ESSID, para la generación de claves genéricas. • Actualizar el Firmware de los dispositivos de comunicación y los parches de seguridad.
24	Incorrecto mantenimiento de la red inalámbrica	Inadecuado control en los mantenimientos de la red.	16/ Muy Grave	• Preparar un cronograma de actividades que incluya: plan de mantenimiento de equipos, seguridad de activos de la red inalámbrica. • Realizar mantenimiento preventivo a la red de la Institución cada 3 meses. • Mantener un inventario de los dispositivos actualizado, controlando su tiempo de uso. • Actualizar el diagrama de red de la Institución. • Capacitar al administrador de red sobre equipos existentes y nuevos. • Instalar correctamente equipos de comunicación usando normas internacionales y con personal capacitado. • Adquirir equipos de marcas reconocidas para optimizar el funcionamiento de la red Wifi.
25		Susceptibilidad del equipamiento a la humedad y	16/ Muy Grave	• Realizar mantenimiento preventivo de los equipos y la red de la Institución cada 3 meses.

		contaminación.		• Evitar el uso de líquidos o contaminantes sobre los dispositivos de comunicación. • Evitar la acumulación de polvo que genere humedad sobre los dispositivos. • Ubicar los dispositivos en lugares elevados, secos y seguros. • Mantener un óptimo control de la temperatura y la humedad, para proteger los activos de la información.
26	Ingeniería social	Acceso No autorizado e intercepción de tráfico.	25/ Muy Grave	• Limitar el acceso a las interfaces administrativas, sólo a través de la red cableada o únicamente a una serie de IPs reservadas. • Establecer el tipo de cifrado WPA2 con el algoritmo de encriptación AES CCMP. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa. • Verificar que el firmware del AP esté actualizado a su última versión con los últimos parches de seguridad. • Cambiar las contraseñas por defecto para el acceso a las interfaces administrativas 1 vez cada mes, por otras más robustas (12 caracteres mínimo, incluyendo letras mayúsculas, números y símbolos especiales). • Evaluar si sería mejor optar por implantar una solución RADIUS. • Mantener un log de eventos de todo lo que ocurre en el AP para detectar cualquier intrusión o intento de explotar una vulnerabilidad. • Tener precaución sobre el uso de los correos electrónicos, al seguir enlaces de contactos conocidos y descargar archivos.

				• Mantener actualizado el sistema operativo y los antivirus en todos los dispositivos. • En caso de disponer de un portal cautivo para el acceso a la red, es imprescindible verificar que los controles de seguridad están implementados correctamente de forma que no sea posible saltarse la autenticación. • Ocultar el nombre que identifica a las redes Wifi de la Institución. • Navegar por páginas web seguras y de confianza, que tengan algún sello o certificado garantizando su calidad y fiabilidad. • Capacitar al personal de la Institución sobre estrategias para prevenir la ingeniería social.
27	Intercepción de información	Intercepción de credenciales de autenticación.	20/ Muy Grave	• Establecer un Wifi IDS que alerte y prevenga cuándo se reciben varios de estos frames, evitando que el AP llegue a procesarlos. • Cambiar la dirección MAC asociada al AP, siempre que los parámetros de configuración del mismo lo permitan. • Disponer de algún sistema de protección ante ataques de fuerza bruta, así como una buena política de contraseñas, para dificultar los ataques basados en diccionario. • Dependiendo del sistema que haya detrás del RADIUS para autenticar a los usuarios, se puede escoger una solución, como por ejemplo un firewall a nivel de base de datos o un IDS. • Utilizar mecanismos de autenticación robustos, como WPA2-CCMP, no utilizar

				credenciales genéricas o predecibles y habilitar la renovación automática de claves. • Deshabilitar el soporte de WPS PIN y verificar que dicha funcionalidad no se encuentra activa.
28	Robo común	Acceso a las instalaciones y equipos inalámbricos.	25/ Muy Grave	• Colocar letreros que impidan el acceso a las instalaciones y equipos inalámbricos. • Realizar mantenimiento preventivo a las cámaras de videovigilancia y la red de la Institución cada 3 meses. • Incrementar cámaras de videovigilancia para interiores y exteriores en la Institución. • Controlar la entrada y salida de las personas a la Institución, manteniendo un registro actualizado. • Ubicar un guardia de seguridad en la Institución; mismo que deberá ser altamente confiable y no registrar antecedentes penales. • Mantener un lugar físico externo adecuado para resguardar copias de seguridad de documentos, sistemas, y demás información de la Institución. • Implementar un sistema de alarmas si el caso lo amerita. • Reforzar puertas y ventanas de la Institución, a fin de evitar el fácil ingreso y robo de equipos informáticos. • Contar con los números telefónicos de: policía nacional, guardias de seguridad, y personal de la Institución. • Contar con un carnet de identificación, siempre en un lugar visible por parte del personal de la Institución. • Contar con pólizas de seguros para los equipos de cómputo.

				• Prohibir facilitar información confidencial de la Institución. • Establecer políticas de autorización de acceso físico a los equipos de cómputo.
29	Virus	Daño de la información.	6/ Apreciable	• Instalar antivirus originales y mantenerlo actualizado. • Evaluar si es posible implementar un sistema IDS o IPS. • Impedir el uso de memorias USB, CD a personal No autorizado por el administrador de red. • Realizar respaldos de la información más importante de los equipos al menos 1 vez por día. • Establecer políticas de seguridad para evitar el uso de aplicaciones no autorizadas o de origen desconocido en las estaciones de trabajo. • Establecer políticas para navegación por Internet y descargas de aplicaciones e información. • Efectuar la depuración de archivos en los discos duros al menos 1 vez cada mes. • Contar con equipos de respaldo ante posibles fallas, para su reemplazo provisional mientras se procede a la desinfección y habilitación • Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran. • Navegar por páginas web seguras y de confianza, que tengan certificado garantizando su calidad y fiabilidad.
Promedio				

Fuente: Autoría Propia

5.2. Análisis de Factibilidad

El análisis de factibilidad es una herramienta que permite considerar los recursos, costos, y el tiempo necesario, para verificar la viabilidad de las actividades que propone el plan de mitigación y que ayudarán en la toma de decisiones a la Institución. Dentro de esta fase se realizarán 3 análisis: técnico, operativo y económico.

5.2.1. Análisis Técnico

Durante este análisis se consideran los recursos humanos (conocimientos y habilidades), técnicos (equipos y herramientas) y el tiempo requerido. La Tabla 28, presenta el análisis de factibilidad técnica para el proyecto.

Tabla 28: Factibilidad Técnica

Recurso Humano	Recurso Técnico	Tiempo
• Administrador de Red.	• Revisión de Documentación: Metodología ISSAF, OWISAM, OSSTMM. • Revisión de Estándar Internacional ISO/IEC 27002:2013.	1 mes
	• Proyecto (Pruebas, Análisis de riesgos, Plan de Mitigación de Riesgos).	5 meses
	• Equipo Tecnológico (Portátil, memorias USB, Impresora, etc.)	-
Total		**6 meses**

Fuente: Autoría Propia

5.2.2. Análisis Operativo

Durante este análisis se verifica que el personal seleccionado para llevar a cabo el proyecto esté debidamente capacitado, y cuente con la experiencia necesaria para ejecutar el plan de mitigación. Debido a la importancia de la implementación del proyecto es necesario que el Administrador de red, este capacitado en:

- Metodología ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información).
- Controles OWISAM (Metodología Abierta para el Análisis de Seguridad Wireless).
- Metodología OSSTMM (Manual de la Metodología Abierta de Comprobación de Seguridad).
- Estándar Internacional ISO/IEC 27002:2013 (Sistemas de Gestión la Seguridad de la Información).
- Herramientas para Hacking Ético (Sistemas y Aplicaciones de libre distribución).
- Infraestructura de Redes y Comunicación Inalámbrica.

5.2.3. Análisis Económico

Durante este análisis se establecen los costos necesarios para el desarrollo del proyecto. La Tabla 29, contiene el detalle de la factibilidad económica.

Tabla 29: Factibilidad Económica

Recurso	Descripción	Meses	Unid	Valor	Total
Humano	Auditor de Seguridad Informática.	6	1	$ 1.500,00	$ 9.000,00
Total Recurso Humano					**$ 9.000,00**
Técnico	Computador Portátil	-	1	$ 750,00	$ 750,00
	Adaptador Wifi Belkin	-	1	$ 25,00	$ 25,00
	Impresora	-	1	$ 350,00	$ 350,00
	Internet, Luz, Teléfono.	6	-	$ 70,00	$ 420,00
	Materiales y Suministros	6	-	$ 25,00	$ 150,00
	Documentación de Metodologías: ISSAF, OWISAM, OSSTMM	1	3	$ 0,00	$ 0,00
	Documentación de la Norma ISO/IEC 27002:2013 (Tecnología de la información-Técnicas de seguridad-Código de prácticas para los controles de seguridad de la información) ***Referencia:*** **www.iso.org**	1	1	$ 178,00	$ 178,00
	Herramientas para Hacking ético.	-	-	$ 0,00	$ 0,00
Total Recurso Técnico					**$ 1873,00**
Total Final					**$10.873,00**

Fuente: Autoría Propia

El costo total del proyecto es **$ 10.873,00**. Las metodologías ISSAF, OWISAM y OSSTMM no presentan costo alguno puesto que son de acceso público y su documentación se puede descargar a través de sus páginas oficiales. Debido que las herramientas para hacking ético son de libre distribución tampoco tienen un costo. Para el caso de las normas ISO/IEC 27002:2013 se utilizó el valor oficial que corresponde al apartado de *"Código de prácticas para los controles de seguridad de la información",* disponible en la página oficial de ISO. Como recurso humano se usó un valor referencial que corresponde a un Auditor de Seguridad Informática.

5.3. Fase 3: Reportes, Limpieza y Destrucción de Artefactos

Durante esta fase se presenta un reporte o informe técnico de los resultados obtenidos en las pruebas de seguridad inalámbrica establecidas por los controles OWISAM. Es importante informar cualquier situación crítica encontrada durante las pruebas para que la Institución tenga constancia, buscando contramedidas para resolver los problemas críticos.

Este informe deberá tener una estructura bien definida siendo: resumen de la servicio, alcance, herramientas, fechas y horas de las pruebas realizadas.

Cabe destacar que la información que se crea en los sistemas de prueba deberá ser removida de éstos. En esta fase la metodología OSSTMM contribuye sobre las recomendaciones para la elaboración del informe técnico, mientras que la metodología ISSAF organiza y planifica la entrega de los resultados en las siguientes actividades:

- Reportes.
- Limpieza y Destrucción de Artefactos.

5.3.1. Reportes y Presentación

Para desarrollar esta actividad; en primera instancia se planifica las tareas que se deben realizar siendo: organizar y controlar la documentación del reporte, y preparar una reunión de trabajo con el equipo de auditoría. En segunda instancia se realiza un análisis de las amenazas y vulnerabilidades encontradas, además de las recomendaciones para mitigar los riesgos y su efectividad. Y finalmente se crea el informe final que según ISSAF tiene la siguiente estructura:

- Resumen.
- Alcance del proyecto.

- Objetivos.
- Cronograma de actividades.
- Pruebas de seguridad realizadas (herramientas).
- Resumen de los resultados obtenidos (amenazas y vulnerabilidades).
- Análisis de Riesgos.
- Plan de Mitigación de riesgos (controles y Recomendaciones).

Después de la elaboración del informe técnico, se debe preparar la presentación con el equipo de auditoria y el Representante legal de la Institución. Esta presentación debe incluir gráficos y gran cantidad de información organizada en tablas, se deberá discutir los descubrimientos y las recomendaciones analizadas.

5.3.2. Limpieza y Destrucción de Artefactos

La información generada durante las pruebas de seguridad, deberá ser removida de los sistemas, además se guardará extrema confidencialidad de la información sensible.

CAPÍTULO 6

ANÁLISIS DE RESULTADOS

En este Capítulo se analizan y comparan los resultados obtenidos con la realización del análisis de riesgos.

6.1. Resultados Obtenidos

Luego de la ejecución de las pruebas de seguridad sobre la red inalámbrica de la Institución, se procedió con el análisis, estimación y evaluación de riesgos determinando un total de 14 amenazas y 29 vulnerabilidades.

Estas vulnerabilidades fueron clasificadas mediante un nivel de riesgo, dando como resultado en términos porcentuales los siguientes valores: 58,62% de vulnerabilidades son de nivel Muy Grave, 37,93% con nivel Importante, 3,45% con nivel Apreciable y 0% con un nivel Marginal como lo muestra la Tabla 30 y la Figura 6.1.

Tabla 30: Resultados Generales del Análisis de Riesgos

Nivel de Riesgo	Cantidad	Porcentaje
Muy Grave	17	58,62%
Importante	11	37,93%
Apreciable	1	3,45%
Marginal	0	0,00%
Total	**29**	**100,00%**

Fuente: Autoría Propia

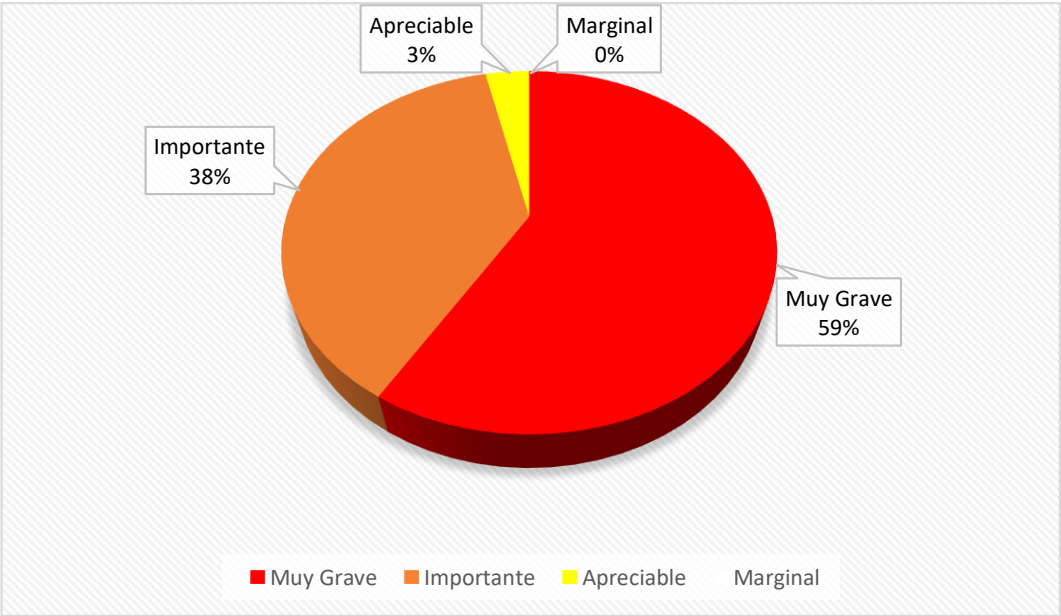


Figura 6.1: Resultado General de Análisis de Riesgos

Fuente: Autoría Propia

6.2. Comparación de Riesgos

En la Tabla 31, se detalla la comparación del análisis de riesgos antes y después de la implementación del plan de mitigación. Debido que es la primera vez que se realiza este análisis y basado en los controles que presenta la Institución; los riesgos antes de la implementación del Plan se ubican en: 17 vulnerabilidades con un nivel Muy Grave, 11 con un nivel Importante, 1 con un nivel Apreciable y no existen vulnerabilidades de tipo Marginal; siendo muy peligroso para los activos de la información.

Con la implementación del plan de mitigación y basados en las recomendaciones sugeridas por la Norma ISO/IEC 27002:2013, los controles OWISAM, y los resultados de la tesis "*Aplicación de hacking ético para la determinación de amenazas, riesgos y vulnerabilidades de la red inalámbrica de una institución, en 2015*"; es posible estimar una reducción del nivel de riesgo sobre cada vulnerabilidad, obteniendo: 11 vulnerabilidades con un nivel de riesgo Apreciable y 18 con un nivel Marginal, eliminando los niveles de tipo Muy Grave e Importante.

Tabla 31: Comparación de Riesgos Antes y Después del Plan de Mitigación

	Antes				Después			
Vulnerabilidad	Muy Grave	Importante	Apreciable	Marginal	Muy Grave	Importante	Apreciable	Marginal
Acceso No autorizado a redes Wifi.	X						X	
Lluvias, rotura de tuberías		X						X
Emisión de señal de clientes no autorizados.	X							X
Ataques de disponibilidad del servicio.		X					X	
Descubrimiento de información de la red Wifi.		X						X
Intercepción de la comunicación.	X						X	
Obtención de información sobre hardware y software.		X						X
Obtención de puertos, servicios y protocolos habilitados.		X					X	
Configuración de dispositivos incorrecta.	X							X
Credenciales débiles.	X							X
Falta de políticas de configuración de dispositivos.	X							X
Falta de políticas de gestión y cambio de claves	X							X
Falta de políticas de uso y restricción de la red Wifi.	X							X

Falta de inventario de dispositivos actualizado.	X							X
Tiempo de vida de contraseñas elevado.	X							X
Obtención de información sensible.	X							X
Engaño o estafa.		X					X	
Falta de políticas de acción contra fuego.		X						X
Acceso a recursos de la red.		X					X	
Acceso a la administración de dispositivos usando Gateway predeterminado.		X					X	
Área de cobertura excesiva.		X						X
Direcciones IPs evidentes al mapear saltos de red.		X					X	
Mecanismo de autenticación WPS habilitado.	X							X
Inadecuado control en los mantenimientos de la red.	X							X
Susceptibilidad del equipamiento a la humedad y contaminación.	X							X
Acceso No autorizado e intercepción de tráfico.	X						X	
Intercepción de credenciales de autenticación.	X						X	

Acceso a las instalaciones y equipos inalámbricos.	X						X	
Daño de la información.			X					X
Total	**17**	**11**	**1**	**0**	**0**	**0**	**11**	**18**

Fuente: Autoría Propia

Comparación Porcentual de Riesgos:

Según la Figura 6.2 y la Tabla 32, los valores porcentuales del nivel de riesgo después de la implementación del plan de mitigación serian: 0% tanto para el nivel de riesgo Muy Grave como para el nivel Importante; 37,93% de los riesgos ahora serian de tipo Apreciable y finalmente el 62,07% estarían dentro del grupo Marginal.

Con la obtención de estos valores es posible garantizar la seguridad y correcto funcionamiento de la red inalámbrica, gestionando de mejor forma los activos de información y verificando que los controles y las recomendaciones proporcionados en el plan de mitigación sean implementadas y actualizadas periódicamente por el responsable de la red de la Institución.

Tabla 32: Comparación General de Riesgos

	Antes		Después	
Nivel de Riesgo	**Cantidad**	**Porcentaje**	**Cantidad**	**Porcentaje**
Muy Grave	17	58,62%	0	0,00%
Importante	11	37,93%	0	0,00%
Apreciable	1	3,45%	11	37,93%
Marginal	0	0,00%	18	62,07%
Total	**29**	**100,00%**	**29**	**100,00%**

Fuente: Autoría Propia

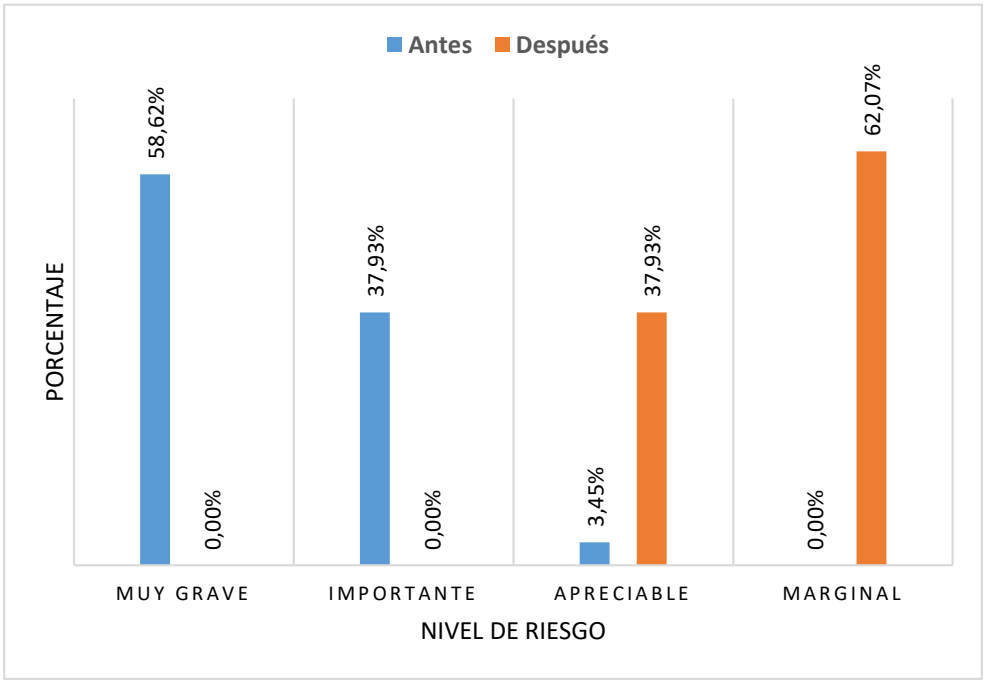


Figura 6.2: Comparación General de Riesgos

Fuente: Autoría Propia

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

1. Durante la fase de evaluación de riesgos se determinó un alto porcentaje de vulnerabilidades con niveles de tipo “Muy grave” e “Importante”.

2. La Institución no cuenta con políticas para la gestión de la seguridad inalámbrica.

3. Se pudo evidenciar que existen fallas en los controles de acceso a la red inalámbrica y los dispositivos.

4. No se realizan capacitaciones a los usuarios sobre seguridad informática.

5. Los usuarios y clientes son susceptibles a ataques de ingeniería social.

Recomendaciones:

1. Se recomienda aplicar las recomendaciones del plan de mitigación con el objetivo de reducir los riesgos y ubicarlos en los niveles “Apreciable” y “Marginal”.

2. Implementar y mantener actualizadas políticas para gestión de claves, uso y restricción de la red inalámbrica y configuración de los dispositivos.

3. Incrementar políticas y procedimientos para controles de acceso a la red inalámbrica y los dispositivos.

4. Realizar capacitaciones periódicas al personal de la Institución sobre seguridad informática.

5. Se recomienda ejecutar los controles del plan de mitigación y mantener cuidado sobre el uso inadecuado de sitios web y correos electrónicos.

BIBLIOGRAFÍA

[1] K. Astudillo, *Hacking Etico 101: Como Hackear Profesionalmente En 21 Dias O Menos!* Createspace Independent Pub, 2013.

[2] eHack, «Las fases del Hacking Ético», *Ethical Hack*, 28-may-2017. .

[3] D. Benchimol, *Hacking Desde Cero*, 2011 edition. Creative Andina Corp., 2011.

[4] «Seguridad Informatica / Políticas de Seguridad de la Información». [En línea]. Disponible en: https://www.segu-info.com.ar/politicas/polseginf.htm. [Accedido: 04-abr-2018].

[5] «SEGURIDAD INFORMÁTICA». [En línea]. Disponible en: http://www.eumed.net/rev/cccss/21/oocs.html. [Accedido: 30-jun-2017].

[6] H. Jara y F. G. Pacheco, *Ethical hacking 2.0: Manuales Users*. Creative Andina Corp., 2012.

[7] «ISSAF - Enciclopedia Secure Arco». [En línea]. Disponible en: http://www.securearc.com/wiki/index.php/ISSAF. [Accedido: 01-jul-2017].

[8] «CIBERNOTICIA # 48 - PENTESTING | Servicios Computacionales Progress». [En línea]. Disponible en: http://www.scprogress.com/cinco/?q=cibernoticia_48. [Accedido: 07-abr-2018].

[9] «OWISAM». [En línea]. Disponible en: https://www.owisam.org/es/P%C3%A1gina_principal. [Accedido: 03-jul-2017].

[10] «ISECOM - Open Source Security Testing Methodology Manual (OSSTMM)». [En línea]. Disponible en: http://www.isecom.org/research/osstmm.html. [Accedido: 03-jul-2017].

[11] «ISO 27002». [En línea]. Disponible en: https://iso27002.wiki.zoho.com/. [Accedido: 04-jul-2017].

[12] D. Benchimol, «Linux Desde Cero», *Librerï¿½as El Sï¿½tano*. [En línea]. Disponible en: https://www.elsotano.com/libro-linux-desde-cero-users-10448205. [Accedido: 19-abr-2018].

[13] «Kali Linux - Penetration Testing Distribution - Documentation». .

[14] «Guía de referencia de Nmap (Página de manual)». [En línea]. Disponible en: https://nmap.org/man/es/index.html. [Accedido: 04-jul-2017].

[15] «Wireshark | Oficina de Seguridad del Internauta». [En línea]. Disponible en: https://www.osi.es/es/herramientas-gratuitas/wireshark. [Accedido: 04-jul-2017].

[16] «Aircrack-ng». [En línea]. Disponible en: https://www.aircrack-ng.org/doku.php. [Accedido: 05-jul-2017].

[17] Rubén Velasco, «Acrylic WiFi : Análisis de este completo monitor de redes inalámbricas Wi-Fi», *RedesZone*. [En línea]. Disponible en: https://www.redeszone.net/redes/acrylic-wifi/. [Accedido: 05-jul-2017].

[18] J. Andreu, *Redes inalámbricas (Servicios en red)*. Editex, 2011.

[19] C. V. MIRANDA, *Sistemas informáticos y redes locales*. Ediciones Paraninfo, S.A., 2005.

ANEXOS

Anexo 1: Cuestionario de Entrevista

CUESTIONARIO DE ENTREVISTA

Objetivo: Determinar la situación actual de la red inalámbrica de la Institución.

1. ¿Qué tipo de mantenimiento que se brinda a la red inalámbrica?

   Preventivo ☐ Correctivo ☑ Ambos ☐

2. ¿La Institución posee políticas de seguridad para la red inalámbrica?

   Sí ☐ No ☑

3. ¿Se realiza capacitaciones periódicas al personal de TI sobre seguridad de la información?

   Sí ☐ No ☑

4. ¿Cuántos usuarios se conectan diariamente a la red inalámbrica de la Institución?

   De 1 a 15 ☑ De 30 a 50 ☐

   De 15 a 30 ☐ Más de 50 ☐

5. ¿Se realizan cambios periódicos en las contraseñas de los dispositivos de comunicación?

   Sí ☐ No ☑

6. ¿Qué tipo de cifrado utilizan los equipos de comunicación?

   WEP ☐ WPA ☑ WPA2 ☐

7. ¿Se lleva un inventario de los dispositivos de comunicación actualizado?

   Sí ☐ No ☑

Firma: Cecilia Bitar Fecha: 17/02/2018

Anexo 2: Lista Completa de Controles de Verificación OWISAM

Controles OWISAM 2013			
Sección	**Referencia**	**Control**	**Vulnerabilidad**
OWISAM Discovery (OWISAM-DI)	OWISAM-DI-001	Descubrimiento de puntos de acceso.	Existencia de rogue Aps.
	OWISAM-DI-002	Descubrimiento de redes ocultas.	debilidades en el firmware y seguridad por oscuridad.
	OWISAM-DI-003	Identificación pasiva de direcciones MAC de dispositivos.	Dispositivos no autorizados.
	OWISAM-DI-004	Descubrimiento de preferencias de redes conocidas de clientes.	Conexión automática a redes inseguras.
	OWISAM-DI-005	Descubrimiento activo de dispositivos y redes.	Descubrimiento de información.
	OWISAM-DI-006	Identificación de relaciones entre dispositivos.	Descubrimiento de información.
OWISAM Fingerprinting (OWISAM-FP)	OWISAM-FP-001	Identificación del dispositivo.	Obtención de información sobre el hardware y software.
	OWISAM-FP-002	Identificación de funcionalidades soportadas por el dispositivo.	Obtención de información sobre el hardware y software.
	OWISAM-FP-003	Enumeración de mecanismos de autenticación radius (802.1x).	Mecanismos de autenticación inseguros
	OWISAM-FP-004	Detección de Rogue Aps.	Intrusos en redes Wi-Fi.
	OWISAM-FP-005	Pruebas de client isolation.	Ataques a clientes.
	OWISAM-FP-006	Detección de ataques por parte de dispositivos Wi-Fi.	Intrusos en redes Wi-Fi.
Pruebas sobre la autenticación (OWISAM-AU)	OWISAM-AU-001	Detección de protección de acceso basado en MAC.	Autenticación contra redes Wi-Fi.
	OWISAM-AU-002	Pruebas sobre WPS.	Acceso no autorizado a redes Wi-Fi.
	OWISAM-AU-003	Pruebas de downgrade del método de autenticación.	Inseguridad en mecanismos de autenticación.
	OWISAM-AU-004	Captura y cracking de claves transmitidas en el proceso de autenticación.	Credenciales débiles.
	OWISAM-AU-005	Uso de protocolos de autenticación inseguros (FAST-EAP,LEAP,EAP-MD5,...)	Interceptación y descifrado de credenciales.

	OWISAM-AU-006	Pruebas de fuerza bruta de usuarios contraseñas de radius (802.1x)	Credenciales débiles.
	OWISAM-AU-007	Pruebas de fuerza bruta de contraseñas contra el proceso de autenticación (PSK)	Posibilidad de descifrar contraseñas débiles offline.
	OWISAM-AU-008	Debilidades en repositorio de credenciales	Acceso no autorizado y robo de credenciales.
Pruebas de cifrado de comunicaciones (OWISAM-CP)	OWISAM-CP-001	Captura y análisis de tráfico en red abierta.	Transmisión de información sensible.
	OWISAM-CP-002	Descifrado de trafico cifrado	Transmisión de información insegura.
	OWISAM-CP-003	Pruebas de análisis de información transmitida a través de Wireless	Obtención de información sensible.
	OWISAM-CP-004	Análisis de protocolos de cifrado inseguro (WEP, TKIP,...)	Debilidad de seguridad en la red.
	OWISAM-CP-005	Pruebas de renovación de claves de cifrado	Tiempo de vida de claves criptográficas elevado.
	OWISAM-CP-006	Pruebas de re-inyección de tráfico (replay attack, Mic,..)	Suplantación de identidad.
Pruebas de configuración de la plataforma (OWISAM-CF)	OWISAM-CF-001	Identificación de redes Wireless con ESSID genérico.	Suplantación de identidad y ataques basados en memory trading.
	OWISAM-CF-002	Contraseñas genéricas en interfaz administrativa del punto de acceso	Credenciales débiles y acceso no autorizado.
	OWISAM-CF-003	Verificación del nivel de intensidad de señal o área de cobertura.	área de cobertura excesiva.
	OWISAM-CF-004	Análisis del solapamiento de redes en el mismo canal de comunicaciones	Degradación de la calidad del servicio.
	OWISAM-CF-005	Generación de claves en base a algoritmos conocidos	Algoritmos de claves PSK o WPS débiles.
	OWISAM-CF-006	Pruebas sobre Upnp	Redirección de puertos.
Análisis de Infraestructura (OWISAM-IF)	OWISAM-IF-001	Debilidades en el firmware del AP.	Robo de credenciales y acceso no autorizado.
	OWISAM-IF-002	Interfaces administrativas expuestas a la red	Acceso no autorizado e interceptación de tráfico.

	OWISAM-IF-003	Política de firewall incorrecta	Acceso a segmentos de red restringidos.
	OWISAM-IF-004	Controles sobre mecanismos de detección de intrusos.	Ausencia de sistemas de monitorización.
	OWISAM-IF-005	Pruebas de verificación de túneles VPN (sobre redes abiertas...)	Interceptación de comunicaciones
	OWISAM-IF-006	Debilidades en servidor radius	Ejecución remota de código o denegación de servicio.
	OWISAM-IF-007	Vulnerabilidades incubadas	Debilidades en elementos de arquitectura o software.
	OWISAM-IF-008	Gestión (Alta/baja/modificación) de claves y certificados.	Gestión incorrecta de claves de acceso.
	OWISAM-IF-009	Dispositivos de comunicaciones accesible/expuestos físicamente	Acceso no autorizado y modificación de firmware.
	OWISAM-IF-010	Detección y análisis de sistemas Scada.	Acceso a sistemas de control industrial.
Denegación de servicio (OWISAM-DS)	OWISAM-DS-001	Pruebas de deautenticación	Interceptación de credenciales de autenticación.
	OWISAM-DS-002	Saturación del canal de comunicaciones (CTS/RTS, ruido, jammering, ...)	Ataques a la disponibilidad del servicio.
	OWISAM-DS-003	Bloqueo de cuentas de usuario	Bloqueo de cuentas.
	OWISAM-DS-004	Bloqueo de dispositivo de comunicaciones	Suplantación de punto de acceso y DOS.
	OWISAM-DS-005	Pruebas de degradación del canal de comunicaciones	Degradación del servicio.
Pruebas sobre directivas y normativa (OWISAM-GD)	OWISAM-GD-001	Identificación de dispositivos que no cumplen el estándar / propietarios	n/a
	OWISAM-GD-002	Detección de dispositivos emitiendo en frecuencias restringidas.	Emisión de señal no autorizada.
	OWISAM-GD-003	Análisis de la política de uso/restricción de uso de redes inalámbricas	Accesos indebidos.
	OWISAM-GD-004	Análisis de la configuración de dispositivos.	Configuración incorrecta.
	OWISAM-GD-005	Análisis de la política de gestión y cambio de claves	Tiempo de vida de contraseñas elevado.
	OWISAM-GD-006	Verificación de inventario de dispositivos autorizados	Inventario no actualizado.

Pruebas sobre clientes inalámbricos (OWISAM-CT)	OWISAM-CT-001	Pruebas de Rogue Ap y asociación automática	Suplantación de identidad y robo de credenciales.
	OWISAM-CT-002	Analisis de APTs (Advanced Persistent Threats) sobre Wireless.	Existencia de ataques persistentes.
	OWISAM-CT-003	Desbordamiento de buffer en cliente.	Ausencia de parches de seguridad y ejecución remota de código.
	OWISAM-CT-004	Extracción de identificadores de usuarios (802.1x)	Recopilación de información y configuración insegura.
	OWISAM-CT-005	Pruebas sobre suplicant débil o inseguro.	Ausencia de validación de certificados.
	OWISAM-CT-006	Ataques contra clientes	Modificación de respuestas DNS,..
	OWISAM-CT-007	Extracción de credenciales de los clientes	Suplantación de identidad.
Pruebas sobre Hotspots / portales cautivos (OWISAM-HS)	OWISAM-HS-001	Acceso a otros segmentos de red sin autenticación	Segmentación o política de cortafuegos incorrecta
	OWISAM-HS-002	Debilidades en el mecanismo de autenticación.	Acceso no autorizado.
	OWISAM-HS-003	Pruebas de encapsulación de tráfico con el exterior	Evasión del mecanismo de autenticación.
	OWISAM-HS-004	Debilidades en portal captivo	Acceso no autorizado.

Anexo 3: Lista Completa de las Secciones de Seguridad OSSTMM

ISECOM Institute for Security and Open Methodologies

OSSTMM – Manual de Metodología Abierta de Testeo de Seguridad

Sección A - Seguridad de la Información

1. Revisión de la Inteligencia Competitiva
2. Revisión de Privacidad
3. Recolección de Documentos

Sección B - Seguridad de los Procesos

1. Testeo de Solicitud
2. Testeo de Sugerencia Dirigida
3. Testeo de las Personas Confiables

Sección C - Seguridad en las tecnologías de Internet

1. Logística y Controles
2. Sondeo de Red
3. Identificación de los Servicios de Sistemas
4. Búsqueda de Información Competitiva
5. Revisión de Privacidad
6. Obtención de Documentos
7. Búsqueda y Verificación de Vulnerabilidades
8. Testeo de Aplicaciones de Internet
9. Enrutamiento
10. Testeo de Sistemas Confiados
11. Testeo de Control de Acceso
12. Testeo de Sistema de Detección de Intrusos
13. Testeo de Medidas de Contingencia
14. Descifrado de Contraseña
15. Testeo de Denegación de Servicios
16. Evaluación de Políticas de Seguridad

Sección D - Seguridad en las Comunicaciones

1. Testeo de PBX
2. Testeo del Correo de Voz
3. Revisión del FAX
4. Testeo del Modem

Sección E - Seguridad Inalámbrica

1. Verificación de Radiación Electromagnética (EMR)
2. Verificación de Redes Inalámbricas [802.11]
3. Verificación de Redes Bluetooth
4. Verificación de Dispositivos de Entrada Inalámbricos
5. Verificación de Dispositivos de Mano Inalámbricos
6. Verificación de Comunicaciones sin Cable
7. Verificación de Dispositivos de Vigilancia Inalámbricos
8. Verificación de Dispositivos de Transacción Inalámbricos
9. Verificación de RFID
10. Verificación de Sistemas Infrarrojos
11. Revisión de Privacidad

Sección F - Seguridad Física

1. Revisión de Perímetro
2. Revisión de monitoreo
3. Evaluación de Controles de Acceso
4. Revisión de Respuesta de Alarmas
5. Revisión de Ubicación
6. Revisión de Entorno

Anexo 4: Lista Completa de los Controles ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

ISO27002.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Octubre-2013

Anexo 5: Niveles de Riesgos Agrupados por Categoría