ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Plan de Seguridad Informática mediante metodologías MAGERIT y OSSTMM V3 para tratamiento del riesgo de ataque hombre en el medio en entornos de red IEEE 802.11b/g/n de acceso libre

RICARDO RAMIRO FIALLOS PROAÑO

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

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA – ECUADOR

MAYO DE 2024

DECLARACIÓN DE AUTENTICIDAD Y CESIÓN DE DERECHOS DE AUTOR

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

Firmado electrónicamente por:
RICARDO RAMIRO
FIALLOS PROANO

No. 1803787264

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, titulado **Plan de Seguridad Informática mediante metodologías MAGERIT y OSSTMM V3 para tratamiento del riesgo de ataque hombre en el medio en entornos de red IEEE 802.11b/g/n de acceso libre**, de responsabilidad del señor **RICARDO RAMIRO FIALLOS PROAÑO** ha sido minuciosamente revisado por los Miembros del Tribunal del Trabajo de Titulación, el mismo que cumple con los requisitos científicos, técnicos, legales, en tal virtud el Tribunal autoriza su presentación.

Ing. Juan Mario Vargas Guambo, Mgtr.
PRESIDENTE

Firmado electrónicamente por:
JUAN MARIO VARGAS GUAMBO

Ing. Sergio Sirilo Gancino Lara, Mgtr.
TUTOR

Firmado electrónicamente por:
SERGIO SIRILO GANCINO LARA

Ing. Jairo Rene Jacome Tinoco, Mgtr.
MIEMBRO

Firmado electrónicamente por:
JAIRO RENE JACOME TINOCO

Ing. Alexandra Orfelina Pazmiño Armijos, Mgtr.
MIEMBRO

Firmado electrónicamente por:
ALEXANDRA ORFELINA PAZMINO ARMIJOS

Mayo de 2024

DEDICATORIA

Primero a Dios, por permitirme culminar este proceso de arduo trabajo. A mi esposa y mis hijos por ser el motor que me impulsa cada día. A mis padres y hermanos por su constante voz de aliento.

AGRADECIMIENTOS

A los docentes y compañeros de aula, por la predisposición de compartir sus conocimientos. A mi tutor y lectores sin su guía esta meta no habría llegado a buen término. A mi esposa, por hacer de esta su meta y doblar esfuerzos para conseguirla.

TABLA DE CONTENIDO

RESUMEN xiv
SUMMARY xv

CAPÍTULO I

1. INTRODUCCIÓN 1
1.1. Planteamiento del problema 1
1.2. Situación problemática 1
1.3. Formulación del problema 2
1.4. Preguntas directrices o específicas de la investigación 2
1.5. Justificación de la investigación 3
1.6. Objetivo general 3
1.7. Objetivos específicos 3
1.8. Hipótesis 4
1.8.1. Hipótesis general 4

CAPÍTULO II

2. MARCO TEÓRICO 5
2.1. Antecedentes del problema 5
2.1.1. Seguridad del estándar IEEE 802.11 5
2.1.1.1. Pre-RSN 5
2.1.1.2. RSN Security 5
2.1.2. Catálogo de amenazas de ataques en el estándar 802.11 6
2.1.3. Ataques de hombre en el medio MiM 7
2.1.3.1. Spoofing-based MiM 8
2.1.3.2. SSL/TLS MiM 8
2.1.3.3. BGP MiM 8
2.2. Bases teóricas 8
2.2.1. Método de análisis de riegos según metodología Magerit 8
2.2.1.1. Identificación de los activos de información 10
2.2.1.2. Identificación de las amenazas 12
2.2.1.3. Determinación de las salvaguardas 14
2.2.1.4. Estimación del impacto residual 16
2.2.1.5. Estimación del riesgo residual 16

2.2.2. Metodología de pruebas de seguridad OSSTMM V3 17
2.2.2.1. Prueba de seguridad 17
2.2.2.2. Proceso operativo de prueba de seguridad 18
2.2.2.3. Modelo OpSec 18
2.3. Operacionalización de variables 21
2.4. Matriz de consistencia 21

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN 25
3.1. Tipo y diseño de investigación 25
3.2. Método de investigación 25
3.3. Enfoque de la investigación 25
3.4. Alcance de la investigación 25
3.5. Población de estudio 25
3.6. Unidad de análisis 25
3.7. Selección de la muestra 26
3.8. Técnicas de recolección de datos primarias y secundarias 26
3.9. Instrumentos de recolección de datos primarios y secundarios 26
3.10. Instrumentos para procesar los datos recopilados 26

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN 27
4.1. Recopilación de información 27
4.1.1. Caracterización de los activos 27
4.1.1.1. Identificación de los activos 28
4.1.1.2. Dependencias entre activos 29
4.1.1.3. Valoración de los activos 29
4.1.2. Caracterización de las amenazas 31
4.1.2.1. Identificación de las amenazas 32
4.1.2.2. Valoración de las amenazas 33
4.1.3. Determinación del riesgo potencial 35
4.1.3.1. Determinación del impacto potencial 35
4.1.3.2. Determinación del riesgo potencial 37
4.1.4. Caracterización de las salvaguardas 39
4.2. Test de eficacia del plan de seguridad 40
4.2.1. Definición de la prueba de seguridad 40

4.2.1.1. ¿Qué deseamos proteger? 40
4.2.1.2. Zona de enfrentamiento 40
4.2.1.3. Alcance 40
4.2.1.4. Vectores 41
4.2.1.5. Equipos necesarios para la prueba 41
4.2.1.6. Tipo de prueba 41
4.2.1.7. Marco legal 42
4.2.2. Cálculo del RAV 42
4.2.3. Cálculo del RAVS en escenario sin aplicar el plan de seguridad 42
4.2.3.1. Porosidad u Op-Sec en escenario inicial 43
4.2.3.2. Controles de interacción o Clase A en escenario inicial 43
4.2.3.3. Controles de proceso o Clase B en escenario inicial 44
4.2.3.4. Limitaciones en escenario inicial 44
4.2.3.5. Cálculo de RAVS para escenario inicial 45
4.2.4. Cálculo del RAVS en escenario con el plan de seguridad aplicado 46
4.2.4.1. Porosidad u Op-Sec en escenario con el plan de seguridad aplicado 47
4.2.4.2. Controles de interacción o Clase A en escenario con el plan de seguridad aplicado . 48
4.2.4.3. Controles de proceso o Clase B en escenario con el plan de seguridad aplicado 48
4.2.4.4. Limitaciones en escenario con el plan de seguridad aplicado 49
4.2.4.5. Cálculo de RAVS para escenario con el plan de seguridad aplicado 49
4.2.4.6. Cálculo de la porosidad 49
4.2.4.7. Cálculo de los controles 51
4.2.4.8. Limitaciones 52
4.3. Valoración de Resultados 52
4.3.1. Criterios de valoración 52
4.3.2. Valoración de los riesgos sin plan de seguridad 55
4.3.3. Valoración de los riesgos con plan de seguridad aplicado 57
4.3.4. Riesgo potencial vs. Riesgo residual 58

CAPÍTULO V

5. PROPUESTA 59
5.1. Plan de seguridad 59
5.1.1. Programas de Seguridad 59
5.1.1.1. Programa de instalación y mantenimiento 59
5.1.1.2. Programa configuración de equipos 62
5.1.2. Plan de ejecución 68
5.1.2.1. Diseño e implementación de la infraestructura 68

5.1.2.2. Configuración de equipos 69
5.1.2.3. Revisión y mantenimiento 70
5.1.2.4. Capacitación del personal 70
5.1.3. Riesgo potencial vs riesgo residual 71

CONCLUSIONES 73
RECOMENDACIONES 74
GLOSARIO
BIBLIOGRAFÍA

ÍNDICE DE TABLAS

Tabla 1-2: Catálogo de amenazas 6
Tabla 2-2: Impacto 13
Tabla 3-2: Riesgo 133
Tabla 4-2: Tipos de salvaguardas 14
Tabla 5-2: Eficacia y madurez de las salvaguardas 155
Tabla 6-2: Operacionalización de variables 21
Tabla 1-4: Uso de Internet Encuesta TICs 2017 INEC 30
Tabla 2-4: Valor del activo Información Personal 30
Tabla 3-4: Valor de los activos 31
Tabla 4-4: Identificación de las amenazas 32
Tabla 5-4: Degradación del valor 33
Tabla 6-4: Valoración de las amenazas 34
Tabla 7-4: Valor de los activos 35
Tabla 8-4: Impacto 35
Tabla 9-4: Impacto potencial de las amenazas sobre los activos 36
Tabla 10-4: Riesgo 37
Tabla 11-4: Riesgo potencial de las amenazas sobre los activos 38
Tabla 12-4: Salvaguardas por cada activo 39
Tabla 13-4: Eficacia y madures de las salvaguardas 39
Tabla 14-4: Porosidad para el cálculo de RAV - Escenario inicial 43
Tabla 15-4: Controles de interacción o Clase A - Escenario inicial 43
Tabla 16-4: Controles de proceso o Clase B - Escenario inicial 44
Tabla 17-4: Limitaciones - Escenario inicial 44
Tabla 18-4: Porosidad para el cálculo de RAV - Escenario con el plan de seguridad aplicado 47
Tabla 19-4: Controles de interacción o Clase A - Escenario con el plan de seguridad aplicado 48
Tabla 20-4: Controles de proceso o Clase B - Escenario con el plan de seguridad aplicado 48
Tabla 21-4: Limitaciones - Escenario con el plan de seguridad aplicado 49
Tabla 22-4: Porosidad para el cálculo de RAV 51
Tabla 23-4: Controles Clase A - Cálculo de RAV 51
Tabla 24-4: Controles Clase B - Cálculo de RAV 51
Tabla 25-4: Limitaciones - Cálculo de RAV 52
Tabla 26-4: Probabilidad de ocurrencia 53
Tabla 27-4: Impacto 53

Tabla 28-4: Riesgo 54
Tabla 29-4: Impacto de las amenazas de ataque de hombre en el medio - Sin plan de seguridad 55
Tabla 30-4: Probabilidad de las amenazas de ataque de hombre en el medio - Sin plan de seguridad..... 56
Tabla 31-4: Riesgo de las amenazas de ataque de hombre en el medio - Sin plan de seguridad. 56
Tabla 32-4: Impacto de las amenazas de ataque de hombre en el medio - Con plan de seguridad 57
Tabla 33-4: Probabilidad de las amenazas de ataque de hombre en el medio - Con plan de seguridad..... 58
Tabla 34-4: Riesgo de las amenazas de ataque de hombre en el medio - Con plan de seguridad 58
Tabla 35-4: Riesgo de ataque sin plan de seguridad vs. Riesgo de ataque con plan de seguridad 58
Tabla 36-4: Estimación de costos Programa Implementación y Actualización..... 61
Tabla 37-4: Riesgo potencial de las amenazas sobre los activos 62
Tabla 38-4: Estimación de costos Programa Configuración..... 64
Tabla 39-4: Impacto residual tras la aplicación del Programa configuración de equipos..... 66
Tabla 40-4: Riesgo residual tras la aplicación del Programa configuración de equipos..... 67
Tabla 41-4: Cronograma Diseño e implementación de infraestructura 68
Tabla 42-4: Lista de control Diseño e implementación de infraestructura 68
Tabla 43-4: Cronograma Configuración de equipos..... 69
Tabla 44-4: Lista de control Configuración de equipos..... 69
Tabla 45-4: Cronograma Revisión y mantenimiento 70
Tabla 46-4: Lista de control Revisión y mantenimiento..... 70
Tabla 47-4: Lista de control Capacitación del personal..... 71
Tabla 48-4: Riesgo potencial vs. Riesgo residual 72

ÍNDICE DE FIGURAS

Figura 1-2: Elementos del análisis de riesgos potenciales 10
Figura 2-2: Elementos del análisis de riesgos residual..... 14
Figura 3-2: Ejemplo de un cálculo RAV 20
Figura 1-4: Dependencias entre activos..... 29
Figura 2-4: Diagrama infraestructura inicial 43
Figura 3-4: Cálculo de RAVS - Escenario inicial..... 46
Figura 4-4: Diagrama infraestructura con el plan de seguridad aplicado..... 47
Figura 5-4: Cálculo de RAVS - Escenario con el plan de seguridad aplicado 50

RESUMEN

El presente trabajo de investigación comparó el riesgo de Ataque de Hombre en el Medio en dos entornos de prueba de red WiFi de acceso Libre; uno con la implementación de un Plan de Gestión de Riesgos basado en la metodología Magerit y otro sin ninguna planificación de gestión de riesgos aplicada. Para llevar a cabo esta evaluación, se generó un Plan de Gestión de Riesgos basado en la metodologia Magerit y fue aplicado en uno de los entornos de prueba. Posteriormente, se evaluó el estado de la seguridad utilizando la metodología OSSTMM y se comparó con un entorno de prueba que no tenía el Plan de Gestión de Riesgos aplicado. Los resultados del estudio revelaron que el entorno en el que se aplicó el Plan de Gestión de Riesgos basado en Magerit experimentó mejoras significativas en los parámetros de seguridad evaluados en comparación con el entorno sin un plan de gestión de riesgos. Se pudo concluir que la implementación del Plan de Gestión de Riesgos basado en la metodología Magerit puede reducir efectivamente el riesgo de ataques de hombre en el medio en un entorno de red WiFi de acceso público. Estos resultados resaltan la importancia de la gestión de riesgos como una herramienta esencial para fortalecer la seguridad en entornos vulnerables, como redes WiFi de acceso público, y destacan la eficacia de la metodología Magerit en este contexto.

Palabras claves: SEGURIDAD INFORMÁTICA, RIESGO DE ATAQUE, MANUAL DE METODOLOGÍA DE PRUEBAS DE SEGURIDAD DE CÓDIGO ABIERTO (OSSTMM), METODOLOGÍA MAGERIT, PLAN DE SEGURIDAD

SUMMARY

The current research work compared the risk of Man in the Middle Attack in two Free Access Wi-Fi network test environments; one with the implementation of a Risk Management Plan based on the Magerit methodology and another without any risk management planning applied. To carry out this evaluation, a Risk Management Plan was generated based on the Magerit methodology and was applied in one of the test environments. The security status was then assessed using the OSSTMM methodology and compared to a test environment that did not have the Risk Management Plan applied. The results of the study revealed that the environment in which the Magerit-based Risk Management Plan was applied experienced significant improvements in the evaluated security parameters compared to the environment without a risk management plan. It was concluded that the implementation of the Risk Management Plan based on the Magerit methodology can effectively reduce the risk of man-in-the-middle attacks in a public access Wi-Fi network environment. These results highlight the importance of risk management as an essential tool to strengthen security in vulnerable environments, such as publicly accessible Wi-Fi networks, and highlight the effectiveness of the Magerit methodology in this context.

CAPÍTULO I

1. INTRODUCCIÓN

1.1. Planteamiento del problema

La conectividad al internet se ha convertido en una necesidad de la sociedad, cada vez más sectores de la sociedad, se ven obligados a disponer de una conexión de internet para realizar trámites triviales y de necesidad común, es así que, tanto las instituciones privadas como organismos de estado al reconocer esta necesidad han empezado a poner al servicio de sus comunidades o clientes puntos de acceso inalámbrico al internet.

Lo dicho provoca un beneficio para la sociedad ya que disminuir la brecha de acceso a la información podría generar efectos positivos en el desarrollo social. (MINTEL, 2018a) Pero, que tan seguras (en términos de seguridad de la información) son las redes públicas en el Ecuador, lamentablemente es un dato que al momento se desconoce en el país. De lo que si se dispone al momento son, datos del tipo de uso que las personas dan al internet en redes de acceso público en el país, lo que estimamos puede ser punto de partida para buscar aportar en la seguridad de la información en entornos de red IEEE 802.11b/g/n de acceso libre en el país.

1.2. Situación problemática

En la actualidad el desarrollo tecnológico se ha visto inmiscuido en todos los sectores de la sociedad, siendo así que, en nuestro entorno laboral y personal la necesidad de disponer de una conexión a internet se está convirtiendo en obligatorio; Siendo así que, el no disponer de acceso a internet marca brechas sociales importantes (MINTEL, 2018b).

El gobierno de Ecuador, al reconocer la importancia que tiene el acceso a la información en el desarrollo de la sociedad ha puesto en marcha políticas que buscan ampliar el porcentaje de población con acceso a Internet en el país. Un ejemplo claro de esta iniciativa de gobierno es el CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, que desde el 1 de diciembre del 2016 en su DISPOSICIÓN TRANSITORIA QUINTA establece, “La obligación de las universidades y escuelas politécnicas públicas y privadas de poner a disposición libre y gratuita de la comunidad académica acceso inalámbrico de internet en toda el área de sus sedes y extensiones, así como los gobiernos autónomos descentralizados que deban poner a disposición libre y gratuita de la ciudadanía acceso a internet inalámbrico en los espacios públicos de concurrencia masiva destinados al ocio y entretenimiento” (Nacional, 2016).

Ante lo expuesto anteriormente, las Universidades y Gobiernos Autónomos Descentralizados deberán implementar redes inalámbricas de libre acceso con conectividad a internet y poner estas a disposición de la ciudadanía.

Por diferentes razones el estándar de mayor uso en entornos inalámbricos es el IEEE 802.11b/g/n, que desde su lanzamiento en su primera versión en el año 1997, ha ido evolucionando en sus diferentes versiones en pro de mejorar sus prestaciones en alcance y capacidad.

Al ser el aire el medio de transmisión usado para las comunicaciones inalámbricas, los esfuerzos para mantener la seguridad en dicho entorno de red han generado mecanismos que restringen el acceso a personas fuera del círculo de confianza de las organizaciones propietarias de la red (Plosz et al., 2016a).

En una red inalámbrica abierta el círculo de confianza de ingreso a la red se expande a toda la ciudadanía, dando como resultado un entorno poco confiable para usuarios habituales y un gran atractivo para posibles atacantes.

La falta de esta barrera puede afectar la capacidad de la red para ofrecer niveles aceptables de Confidencialidad, Integridad y Disponibilidad en el medio, por lo que, el objetivo del presente trabajo de investigación busca contribuir a la mejora de la seguridad en dichas circunstancias.

Los ataques de Hombre en el Medio infieren un riesgo mayor en la pérdida de la Confidencialidad e Integridad en entornos wi-fi cerrados. No existen estudios previos que clasifiquen el riesgo que conlleva esta amenaza en redes wifi abiertas (Plosz et al., 2016b).

1.3. Formulación del problema

¿Contribuirá a la reducción del riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre la elaboración de un plan de seguridad informática mediante metodologías Magerit y OSSTMM V3?

1.4. Preguntas directrices o específicas de la investigación

- ¿Cuál es el riesgo inherente de ataque Hombre en el Medio en un entorno de prueba de una red IEEE 802.11b/g/n de acceso libre?

- ¿Qué debe incluir un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3 diseñado para disminuir el riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre?
- ¿Cuál es el riesgo residual de ataque Hombre en el Medio tras la aplicación de un plan de seguridad informática en un entorno de prueba de una red IEEE 802.11b/g/n de acceso libre?

1.5. Justificación de la investigación

El presente trabajo de investigación busca en primer lugar caracterizar el riesgo de ataques de Hombre en el Medio en redes abiertas del estándar IEEE 802.11b/g/n con la finalidad de generar conocimiento que contribuya en mitigar dicho riesgo.

Mediante la aplicación de una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información se desea generar un Plan de Seguridad Propuesto que mitigue el riesgo de este tipo de ataques.

La generación de un plan de seguridad informática beneficiará a las entidades públicas y privadas que administren redes abiertas del estándar IEEE 802.11b/g/n que busquen mecanismos que mitiguen los riesgos en dichos entornos.

La principal importancia de la investigación radica, en que no existen estudios previos que busquen mejorar la seguridad de redes abiertas de dicho estándar, lo que sumado a la popularidad de dicha tecnología de red, podría conllevar a un incremento de redes abiertas del estándar IEEE 802.11b/g/n con graves falencias de seguridad.

1.6. Objetivo general

Generar un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3, para tratar el riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre.

1.7. Objetivos específicos

- Determinar el riesgo inherente de ataque Hombre en Medio en un entorno de prueba de una red IEEE 802.11b/g/n de acceso libre.

- Generar un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3 que trate el riesgo de ataque Hombre en el Medio SSL en entornos de red IEEE 802.11b/g/n de acceso libre.
- Evaluar el riesgo residual de ataque Hombre en el Medio tras la aplicación del plan de seguridad en un entorno de prueba de una red IEEE 802.11b/g/n de acceso libre.

1.8. Hipótesis

1.8.1. Hipótesis general

El uso de un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3, disminuirá el riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes del problema

La revisión bibliográfica del presente trabajo de investigación es amplia. Varios son los estudios relacionados que se han realizado entorno a la seguridad de las comunicaciones inalámbricas y estudios de riesgo de ataque de Hombre en el Medio MiM, por lo que citaremos los estudios que consideramos de mayor relevancia para el alcance de nuestros objetivos.

2.1.1. Seguridad del estándar IEEE 802.11

Con la finalidad de alcanzar los objetivos de la comunicación WLAN el estándar 802.11 propuso WEP (Wired Equivalent Privacy) en 1999 con la finalidad de proveer confidencialidad e integridad de los datos que se transmiten sobre este medio. En 2004, una corrección del estándar fue publicada para mitigar problemas de seguridad, en esta enmienda dos clases de seguridad fueron propuesta:

- Pre-RSN Security
- RSN Security

2.1.1.1. Pre-RSN

Las capacidades de seguridad heredadas desarrolladas en el estándar IEEE 802.11 original. Existen dos tipos:

- Sistema abierto: Este puede ser comprometido por acceso no autorizado con ataques MAC Sppoofing o Rouge AP.
- Autenticación de clave compartida y protección de confidencialidad WEP: Este es tan inseguro como un sistema abierto. Las autenticaciones basadas en WEP pueden ser fácilmente comprometidas con pérdidas de la confidencialidad e integridad de las comunicaciones. El manejo de la clave es otro obstáculo, especialmente en redes de muchos usuarios. Rogue AP, ataques de diccionario, escucha de los paquetes de autenticación y robo de pass key son algunos de los ataques sobre la autenticación de clave compartida.

2.1.1.2. RSN Security

Incluye un número como mecanismo de seguridad para crear una robusta red segura. Dos protocolos de autenticación de origen de la información, chequeo de integridad y confidencialidad fueron propuestos en el estándar 802.11i TKIP y CCMP.

CCMP obedece a FIPS ya que usa un bloque de cifrado AES de 128bits. TKIP tiene vulnerabilidades ya que al igual que WEP usa un bloque de cifrado RC4. WPA puede ser descubierto en menos de un minuto con un ataque de hombre en el medio (Plosz et al., 2016c).

2.1.2. Catálogo de amenazas de ataques en el estándar 802.11

Un catalogó de amenazas recopila una lista de las amenazas conocidas. ¿¿La Tabla ?? muestra una lista de las amenazas de ataques para comunicaciones inalámbricas (Plosz et al., 2016b).

Los ataques activos son aquellos que transmiten o remplazan el tráfico mientras que los ataques pasivos son aquellos que se limitan a escuchar el tráfico (Plosz et al., 2016d).

Las amenazas de ataque de Hombre en el Medio MiM presentan un riesgo potencial Mayor en las dimensiones de seguridad de Confidencialidad, Integridad y Autenticidad (Plosz et al., 2016e).

Tabla 1-2: Catálogo de amenazas

Eavesdropping (ED)	El atacante realiza un monitoreo de las comunicaciones de la red para capturar información y credenciales de autenticación. (pasivo)
Man-in-the-Middle (MiM)	El atacante intercepta la comunicación entre los legítimos participantes para obtener las credenciales de autenticación e información. (activo)
Masquerading (MQ)	El atacante suplanta a un usuario autorizado para obtener ciertos privilegios no autorizados. (activo)
Message Modification (MM)	El atacante altera un mensaje legítimo para borrarlo, modificarlo o reordenarlo. (activo)
Message Replay (MR)	La atacante recepta y retransmite los mensajes actuados como si el atacante fuera el legítimo usuario. (activo y pasivo)
Traffic analysis (TA)	El atacante de manera pasiva realiza monitoreo de las transmisiones para identificar parámetros de la comunicación y sus participantes. (pasivo)
Routing Attack (RA)	Un ataque de capa de red, donde el atacante trata de manipular la tabla de ruteo para redireccionar tráfico en redes WMN y WSN. (activo)

Authentication Attacks (AA)	Intrusos usan este ataque para robar la identidad de usuarios legítimos. Ataques de diccionario y fuerza bruto son ataques comunes en esta categoría. (activo)
Availibility/Denial of Service At-tacks (DoS)	El atacante intenta inhibir o prevenir el uso legítimo de la red inalámbrica. (activo)

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p. 44).
Realizado por: Fiallos, Ricardo, 2022.

2.1.3. Ataques de hombre en el medio MiM

El ataque Man-In-The-Middle (MiM) es uno de los ataques más conocidos en seguridad informática, que representan una de las mayores preocupaciones para los profesionales de seguridad. MiM apunta a los datos reales que fluyen entre los puntos finales y el confidencialidad e integridad de los datos en sí (Conti et al., 2014a).

Este es un tipo de ataque donde un tercero malintencionado toma en secreto el control de canal de comunicación entre dos o más puntos finales.

El atacante MiM puede interceptar, modificar, cambiar o reemplazar el tráfico de comunicación de las víctimas (esto distingue un MiM de un simple espía). Además, las víctimas no son conscientes del intruso, creyendo así que el canal de comunicación está protegido (Conti et al., 2014b).

En particular, el ataque MiM tiene como objetivo comprometer:

- Confidencialidad, escuchando a escondidas la comunicación.
- Integridad, interceptando la comunicación y modificando mensajes
- Disponibilidad, interceptando y destruyendo mensajes o modificar mensajes para que una de las partes finalice comunicación.

Podemos identificar al menos tres formas de caracterizar los ataques de Hombre en el medio:
1) MiM soportado en técnicas de suplantación.
2) MiM soportado en el canal de comunicación en el que el ataque se ejecuta.
3) MiM soportado en la ubicación del atacante y el objetivo en la red (Conti et al., 2014b).

Esta clasificación divide los ataques MiM según el enfoque que usa el atacante para convencer a las víctimas de que son puntos finales válidos, lo que permite enfocarse completamente en el ataque. Ademas resulta de utilidad recopilar los aspectos débiles y fuertes de los algoritmos a

través de diferentes canales de comunicación con la finalidad de que los investigadores puedan encontrar las medidas que se deben tomar para disminuir el riesgo de que un ataque de MiM se materialice en la red que protegemos. Visto desde esta perspectiva los ataques MiM se pueden dividir en (Conti et al., 2014c):

2.1.3.1. Spoofing-based MiM

Este tipo de ataque intercepta la información de una comunicación legítima entre dos usuarios, ejerciendo control en el flujo de la información que se transmite, esto mientras el o los usuarios no se percatan de que están siendo atacados, este tipo de ataques se puede realizar en el dispositivo que sirve de conexión entre las víctimas o directamente en el dispositivo de la víctima (Conti et al., 2014c).

2.1.3.2. SSL/TLS MiM

Es un ataque de red activo, donde el atacante intercepta la comunicación entre un usuario y un servidor, usualmente un servidor web. Luego el atacante genera dos comunicaciones SSL una con la víctima y otra con el servidor, este ataque permite al intruso tener acceso a todos los mensajes que las victimas piensan que viajan cifrados (Conti et al., 2014c).

2.1.3.3. BGP MiM

Este tipo de ataque se realiza tras un secuestro de IP, luego el atacante retransmite el tráfico robado hacia una Estación Autónoma propiedad del atacante donde la información es manipulada (Conti et al., 2014c).

2.2. Bases teóricas

2.2.1. Método de análisis de riegos según metodología Magerit

El uso de tecnologías de la información y comunicaciones (TIC) supone beneficios para los ciudadanos; desafortunadamente dan lugar también a ciertos riesgos, los mismos que deben ser gestionados con medidas de seguridad que generen confianza en los usuarios.

En respuesta a dicha necesidad el organismo de control europeo CSAE (Consejo Superior de Administración Electrónica) elaboró Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) como una guía de gestión para organismos públicos y privados que depende de los sistemas de información para alcanzar sus objetivos.

La terminología de Magerit sigue la normativa ISO 31000, y desarrolla el marco del Proceso de Gestión de Riesgos, lo que permite integrarla al Marco de trabajo para la gestión de riegos de la ISOO 31000, dándole a las organizaciones la posibilidad de tomar decisiones teniendo en cuenta los riesgos inherentes en las tecnologías de la información (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012i). La aplicación de Magerit busca:

- Crear conciencia en los responsables de sistemas de información sobre la existencia de riesgos y la necesidad de gestionarlos.
- Poner a disposición un método ordenado para analizar los riesgos que se producen tras el uso de las TIC.
- Ser una guía de ayuda para descubrir los riesgos en los sistemas de información y tratar los mismos de manera oportuna (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012i).

Para llegar a estos objetivos Magerit divide la Gestión de Riesgos en dos tareas principales:

- El análisis de riesgos
- El tratamiento de los riesgos

Para determinar los riesgos Magerit sigue los siguientes pasos:

1) Caracterizar los activos, que relevancia tienen en la organización, el valor que tienen y la dependencia entre activos.
2) Determinar las amenazas que puedan degradar los activos.
3) Determinar las salvaguardias en caso de no tenerlas, si ya existen determinar cuan eficaces son.
4) Estimar el impacto que causaría la materialización de las amenazas sobre los activos.
5) Estimar el riesgo que viene a ser el impacto ponderado con la tasa de ocurrencia de la amenaza.

La Ilustración 1-2 muestra en forma gráfica los pasos detallados:

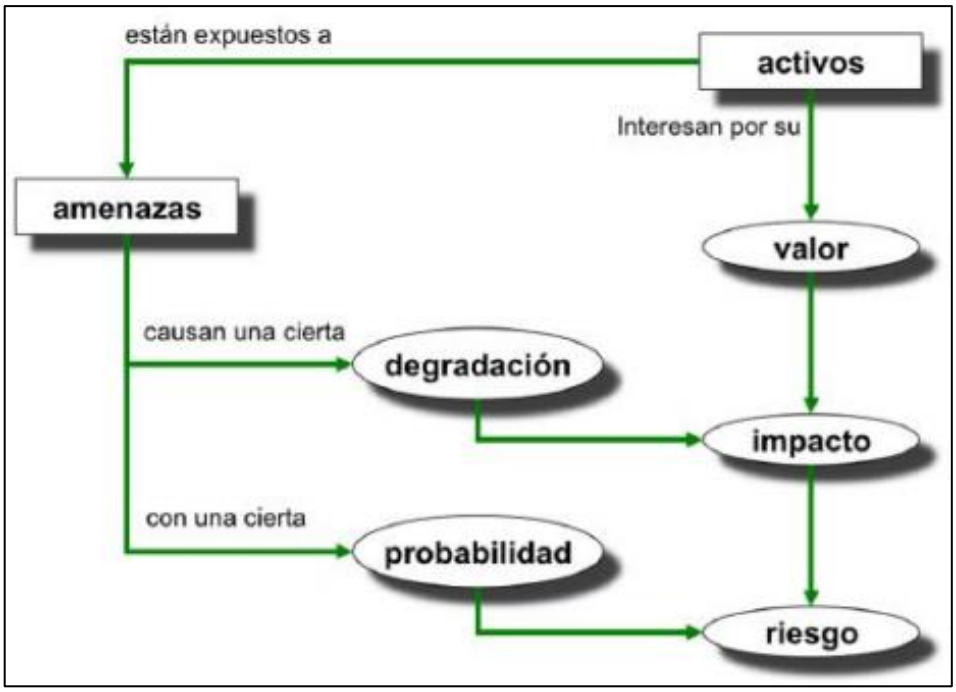

Figura 1-2: Elementos del análisis de riesgos potenciales

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p. 22).

2.2.1.1. Identificación de los activos de información

Los activos son componentes o funcionalidades de un sistema de información que pueden ser atacados de manera intencional o accidental generando un perjuicio a la organización. De los activos nos interesa conocer, cuales son, en qué medida se relacionan y su valor. Dos activos son esenciales en un sistema de información, la información y el servicio, estos marcan los requisitos de seguridad para todo el sistema. El resto de activos se pueden clasificar dentro de datos, aplicaciones, equipos, comunicaciones, recursos físicos y recursos humanos (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012j).

Los activos esenciales dependen de otros activos, de allí que estas dependencias entre activos formen árboles de grafos, en estos árboles de grafos la dependencia entre activos se da de arriba hacia abajo, mientras que la propagación del daño en caso de materialización de las amenazas se da de abajo hacia arriba (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012a).

Tomando en cuenta estas dependencias los árboles de grafos los activos tendrán un valor propio y un valor acumulado, donde el valor de los activos superiores se acumula en los activos inferiores. La valoración de los activos se la realiza en las dimensiones de seguridad, confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012b).

- Confidencialidad: ¿Qué daño causaría que lo conociera quien no debe?
- Integridad: ¿Qué perjuicio causaría que estuviera dañado o corrupto?
- Disponibilidad: ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

En sistemas dedicados a servicios de la sociedad de la información como puedan ser los de administración electrónica o comercio electrónico, el conocimiento de los actores es fundamental para poder prestar el servicio correctamente y poder perseguir los fallos (accidentales o deliberados) que pudieran darse. Así pues, en los activos esenciales, frecuentemente es útil valorar:

- Autenticidad: ¿Qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- Trazabilidad Del uso del servicio: ¿Qué daño causaría no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo?
- Trazabilidad Del acceso a los datos: ¿Qué daño causaría no saber quién accede a qué datos y qué hace con ellos? (Modernización Administrativa and e Impulso de la Administración Electrón, 2012e).

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- Coste de reposición: adquisición e instalación.
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo.
- Lucro cesante: pérdida de ingresos.
- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos, propios o ajenos.
- Daño a personas.
- Daños medioambientales.

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- La homogeneidad: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra.
- La relatividad: es importante poder relativizar el valor de un activo en comparación con otros activos.

Valoración cualitativa: Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

La "Guía de Técnicas" presenta un modelo de análisis basado en valoraciones cualitativas.

Valoración cuantitativa: Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente "natural". La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

- ¿Vale la pena invertir tanto dinero en esta salvaguarda?
- ¿Qué conjunto de salvaguardas optimizan la inversión?
- ¿En qué plazo de tiempo se recupera la inversión?
- ¿Cuánto es razonable que cueste la prima de un seguro?

2.2.1.2. Identificación de las amenazas

Las amenazas son sucesos voluntarios o involuntarios que pueden ocurrir y tras su ocurrencia causar un daño a los activos, las amenazas están clasificadas en desastres naturales, de origen industrial, errores y fallos no intencionados, ataques no intencionados (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012c).

No todas las amenazas afectan a todos los activos y cada amenaza afecta a diferentes parámetros de dimensión de seguridad, cuando hayamos definido que amenazas afectan a que activo y en que dimensión de seguridad debemos valorar la severidad de la afectación que sufriría el activo en

caso de materializarse la amenaza en dos sentidos, la degradación (cuan perjudicado resulta el valor de un activo) y la probabilidad (cuan probable o improbable es que se materialice la amenaza). Conocidas el valor del activo en cada dimensión y la degradación que produce la amenaza lo siguiente es determinar el Impacto Potencial que no es otra cosa que la medida del daño sobre el valor activo derivado de la materialización de la amenaza (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012d).

Para realizar este cálculo podemos hacer uso del Análisis mediante tablas, tomado de Magerit Libro III Guía de técnicas (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012e).

Tabla 2-2: Impacto

		Degradación		
		B	**M**	**A**
Valor	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p. 30).

Realizado por: Fiallos, Ricardo, 2022.

Conocidas el Impacto de las amenazas sobre los activos y la Probabilidad de ocurrencia de la amenaza podemos determinar el Riesgo Potencial, una vez más podremos usar el Análisis mediante tablas, tomado de Magerit Libro III Guía de técnicas (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012e).

Tabla 3-2: Riesgo

		Probabilidad		
		B	**M**	**A**
Impacto	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p. 44).

Realizado por: Fiallos, Ricardo, 2022.

2.2.1.3. Determinación de las salvaguardas

Las medidas del riesgo hasta ahora han sido tomadas en el caso de que no exista ningún control de mitigación. En la práctica no es frecuente encontrar sistemas desprotegidos. Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.

Es importante tomar en cuenta ciertos parámetros al momento de escoger una salvaguarda, factores tales como tipo de activos a proteger, dimensión o dimensiones de seguridad que requieren protección, amenazas de las que necesitamos protegernos, si existen salvaguardas alternativas.

Las salvaguardas entran en el cálculo del riesgo de dos formas, Reduciendo la probabilidad de las amenazas, Limitando el daño causado (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012f).

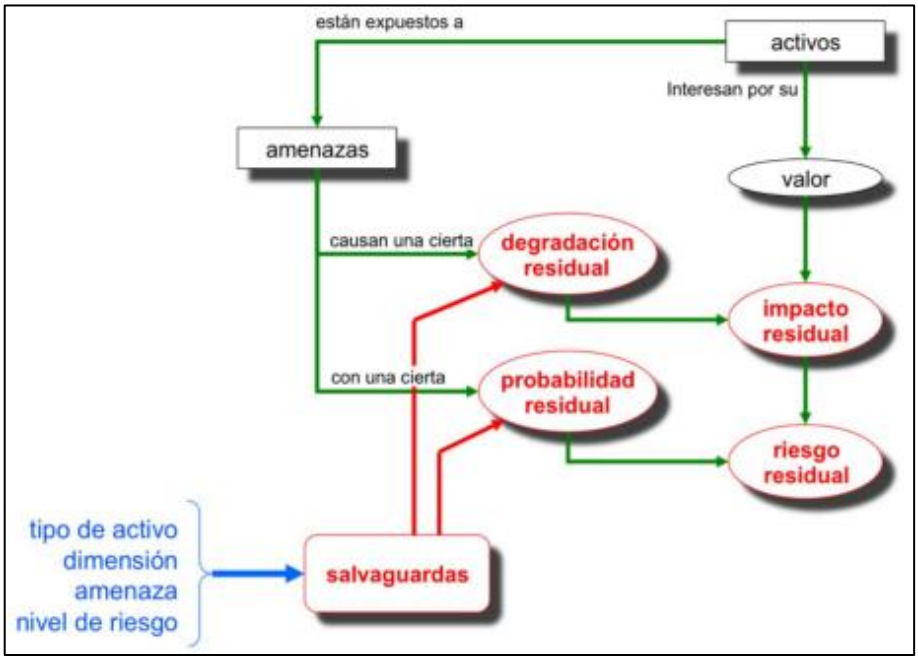

Figura 2-2: Elementos del análisis de riesgos residual

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p. 32).

Magerit relaciona las salvaguardas tomando en cuenta si estas disminuyen la probabilidad o la degradación, como se muestra en la Tabla 4-2:

Tabla 4-2: Tipos de salvaguardas

Efecto	Tipo
Preventivas: Reducen la probabilidad	[PR] Preventivas, [DR] Disuasorias, [EL] Eliminatoria.
Acotan la degradación	[IM] Minimizadoras, [CR] Correctivas, [RC] Recuperativas.
Consolidan el efecto de las demás	[MN] de monitorización, [DC] de detección, [AW] de concienciación, [AD] administrativas.

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p. 68).
Realizado por: Fiallos, Ricardo, 2022.

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda es ideal, eficacia que combina 2 factores:

Desde el punto de vista técnico:

- Es técnicamente idónea para enfrentarse al riesgo que protege.
- Se emplea siempre.

Desde el punto de vista de operación de la salvaguarda:

- Está perfectamente desplegada, configurada y mantenida.
- Existen procedimientos claros de uso normal y en caso de incidencias.
- Los usuarios están formados y concienciados.
- Existen controles que avisan de posibles fallos.

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012f):

Tabla 5-2: Eficacia y madurez de las salvaguardas

Factor	Nivel	Significancia
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible, pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible

100%	L5	Gestionado y medible

Fuente: Modernización Administrativa and e Impulso de la Administración Electrónica (2012i, p.34)
Realizado por: Fiallos, Ricardo, 2022.

2.2.1.4. Estimación del impacto residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.
El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012g).

2.2.1.5. Estimación del riesgo residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual. La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012h).

2.2.2. Metodología de pruebas de seguridad OSSTMM V3

OSSTMM es una metodología de pruebas de seguridad abierta basada en OpSec Seguridad Operativa por sus siglas en inglés, esta metodología busca determinar si los controles, mecanismos y prácticas implementadas en un sistema de gestión de riesgos funciona de forma idónea y reduce los riesgos en la forma que se espera.

Para ello OpSec identifica la eficacia de la salvaguarda de acuerdo al porcentaje de separación del riesgo con el activo a proteger (ISECOM, 2010a).

2.2.2.1. Prueba de seguridad

La metodología divide la prueba de seguridad en siete pasos, con la finalidad de reducir la complejidad al momento de efectuar la misma. Estos pasos son los siguientes:

1) Defina lo que quiere proteger. Estos son los activos. Los mecanismos de protección son los controles que probará para identificar las limitaciones.
2) Identificar el área alrededor de los activos. Esto incluye los mecanismos de protección y los procesos o servicios construidos alrededor de los activos. Aquí es donde tendrá lugar la interacción con los activos. Esta es la zona de compromiso.
3) Definir segunda zona. Todo lo que se necesita fuera de la zona de participación para mantener los activos operativos. Esto puede incluir cosas que influir directamente también se define lo que mantiene la infraestructura operativa como procesos, protocolos y recursos. Este es el alcance de la prueba.
4) Defina los vectores. Cada Vector será cada forma en la que la información interactúa en los diferentes procesos del rol de negocio. Cada vector idealmente debería ser una prueba.
5) Identificar qué equipo se necesita para cada prueba. Dentro de cada vector, pueden ocurrir interacciones en varios niveles. Estos niveles pueden clasificarse de muchas formas, sin embargo la metodología define cinco canales. Los canales son humanos, físicos, inalámbricos, Telecomunicaciones y redes de datos. Cada canal debe probarse por separado para cada vector.
6) Determina qué información quieres aprender de la prueba. ¿Probará interacciones con los activos o también de las salvaguardas? El tipo de prueba debe ser individualmente definido para cada vector, sin embargo, hay seis tipos comunes identificados aquí como ciego, doble ciego, Caja gris, caja gris doble, tándem y reversión.
7) Definir requerimientos legales de las pruebas. Una directriz para asegurar el proceso de cada prueba de seguridad adecuada sin crear malentendidos, conceptos erróneos o falsas expectativas. El resultado final será una medida de su superficie de ataque. La superficie de ataque es la parte desprotegida. del Alcance de un Vector definido.(ISECOM, 2010b)1. Defina

lo que quiere proteger. Estos son los activos. Los mecanismos de protección son los controles que probará para identificar las limitaciones.

2.2.2.2. Proceso operativo de prueba de seguridad

En la metodología determina los siguientes pasos resumidos de la siguiente manera:

1) Recopile pasivamente datos de operaciones normales para comprender el objetivo.
2) Pruebe activamente las operaciones agitando las operaciones más allá de la línea de base normal.
3) Analizar los datos recibidos directamente de las operaciones probadas.
4) Analizar datos indirectos de recursos y operadores (es decir, trabajadores, programas).
5) Correlacionar y conciliar los resultados de las pruebas de datos directos (paso 3) e indirectos (paso 4) y determinar los procesos de seguridad operacional.
6) Determinar y conciliar errores.
7) Derivar métricas de operaciones tanto normales como agitadas.
8) Correlacionar y reconciliar la inteligencia entre operaciones normales y agitadas (pasos 1 y 2) para determinar el nivel óptimo de protección y control que sería mejor implementar.
9) Asigne el estado óptimo de las operaciones (paso 8) a los procesos (paso 5).
10) Crear un análisis de brechas para determinar qué mejoras son necesarias para los procesos que gobiernan protección y controles necesarios (paso 5) para lograr el estado operativo óptimo (paso 8) del actual (ISECOM, 2010c).

2.2.2.3. Modelo OpSec

Hay dos problemas con un análisis de seguridad en el uso práctico. El primero es que al ser la tecnología tan extensa la capacidad del analista para comprender cómo funciona todo es limitada. El segundo problema es que, irónicamente, la obtención de esta información de cómo funciona algo, incluidos los procesos de los negocios, pueden entrar en ilegalidades. Sin embargo, incluso en los casos en que la tecnología o el proceso no se pueden analizar directamente, el producto se puede analizar en el entorno con el que interactúa.

Para cada vector y canal el analista puede colocar una superposición del modelo OpSec sobre los objetivos. El modelo OpSec es simplemente contar los controles para cada punto interactivo de Acceso o Confianza. El proceso se verá así:

1) ¿Qué es visible en el alcance? ¿Qué es de posible valor que se conoce? ¿Qué objetivo pueden ser determinado?

2) ¿Cuáles son los puntos de acceso interactivos a esos objetivos y de qué vector o canal?
3) ¿Cuáles son los Fideicomisos dentro del alcance y sobre qué vector o canal?
4) ¿Cuáles son los controles para esos Accesos y Fideicomisos?
5) ¿Los controles están completos o tienen limitaciones?

Incluso una aplicación rápida del modelo OpSec dirá si un Access o un Trust está equilibrado con los controles. Esto le dirá el tamaño de la superficie de ataque y qué puntos interactivos están abiertos sin ningún control (ISECOM, 2010d).

Figura 3-2: Ejemplo de un cálculo RAV

Fuente: ISECOM (2010a, p. 67).

2.3. Operacionalización de variables

Tabla 6-2: Operacionalización de variables

VARIABLE	TIPO DE VARIABLE	CONCEPTO	INDICADOR	TÉCNICA	INSTRUMENTO
Riesgo de ataque de hombre en el medio en entornos de redes red IEEE 802.11b/g/n de acceso libre	Dependiente	Probabilidad de materialización de ataques de hombre en medio en entornos de red IEEE 802.11b/g/n de acceso libre	Probabilidad de ocurrencia de ataque de hombre en medio en entornos de IEEE 802.11b/g/n de acceso libre	Método de análisis de riegos	Metodología Magerit
Madurez del plan de gestión del riesgo de ataque de hombre en el medio en entornos de redes red IEEE 802.11b/g/n de acceso libre	Independiente	Nivel del proceso de mejora continua de los controles de un plan de gestión de riesgos	Tipo de nivel de madurez del plan de gestión de riesgos según la metodología Magerit	Método de gestión de riesgos	Metodología Magerit

Realizado por: Fiallos, Ricardo, 2022.

2.4. Matriz de consistencia

Tabla 7-2: Matriz de consistencia

FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	TÉCNICAS	INSTRUMENTOS
¿Contribuirá a la reducción del riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre la elaboración de un plan de seguridad informática mediante metodologías Magerit y OSSTMM V3?	**General** Generar un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3, para tratar el riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre. **Específicos** Determinar el riesgo inherente	El uso de un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3, disminuirá el riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre.	**Variable independiente** Madurez del plan de gestión del riesgo de ataque de hombre en el medio en entornos de redes red IEEE 802.11b/g/n de acceso **Variable dependiente** Riesgo de ataque de hombre en el medio en entornos de redes red IEEE	**Variable independiente** Tipo de nivel de madurez del plan de gestión de riesgos según la metodología Magerit **Variable dependiente** Probabilidad de ocurrencia de ataque de hombre en medio en entornos de IEEE 802.11b/g/n de acceso libre	**Variable independiente** Método de gestión de riesgos **Variable dependiente** Método de análisis de riegos	Metodología Magerit

	de ataque Hombre en Medio en un entorno de prueba de una red IEEE 802.11b/g/n de acceso libre. Generar un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3 que trate el riesgo de ataque Hombre en el Medio SSL en entornos de red IEEE		802.11b/g/n de acceso libre			

	802.11b/g/n de acceso libre. Evaluar el riesgo residual de ataque Hombre en el Medio tras la aplicación del plan de seguridad en un entorno de prueba de una red IEEE 802.11b/g/n de acceso libre.					

Realizado por: Fiallos, Ricardo, 2022.

CAPÍTULO III

3. METODOLOGÍA DE INVESTIGACIÓN

3.1. Tipo y diseño de investigación

El tipo de estudio será casi experimental: Al aplicar los controles del plan de seguridad las variables independientes sufrirán cambios. Los cuáles serán medidos y comparados. El diseño de estudio será longitudinal; Se observan las variables independientes en estado inherente y posterior a la aplicación del plan de seguridad en estado residual.

3.2. Método de investigación

El método de estudio será inductivo: Ya que el estudio propuesto busca, medir la reducción del riesgo de ataque Hombre en el Medio en un entorno específico como método para abordar una problemática general.

3.3. Enfoque de la investigación

Al ser el Riesgo nuestra Variable Dependiente el enfoque de la investigación será Cualitativo, ya que, para medir el riesgo, se utilizará escalas cualitativas de gravedad del mismo.

3.4. Alcance de la investigación

El alcance de la investigación será descriptivo, al recoger información de los activos de información del uso del internet en Ecuador se conocerá el impacto que podría tener un ataque de Hombre en el Medio en redes abiertas del estándar IEEE 802.11b/g/n y Correlacional, al establecer el nivel de reducción del Riesgo, tras la aplicación del plan de seguridad propuesto.

3.5. Población de estudio

Hombres y mujeres del Ecuador de entre 16 a 40 años de edad, que para conectarse a internet usen centros de acceso público.

3.6. Unidad de análisis

Las unidades de análisis son las siguientes:

- Personas que se conectan a internet mediante centros de acceso público.

- Entidades públicas o privadas que disponen de redes de acceso público del estándar IEEE 802.11b/g/n.

3.7. Selección de la muestra

Los datos usados para el presente trabajo de investigación serán extraídos de la base de datos proporcionados por el INEC de la Encuesta Tecnológica TIC-2017.

3.8. Técnicas de recolección de datos primarias y secundarias

Se utilizarán las siguientes técnicas de recolección de datos primarias y secundarias:

- Observación.
- Documental.

3.9. Instrumentos de recolección de datos primarios y secundarios

Los instrumentos de recolección de datos primarios y secundarios serán:

- Formato para observación estructurada.
- Indicadores y estadísticas publicadas por el INEC de la Encuesta Tecnológica TIC-2017.

3.10. Instrumentos para procesar los datos recopilados

Como instrumentos para procesar los datos recopilados se utilizarán:

- Magerit.
- OSSTMM V3.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

Para el desarrollo del Plan de seguridad, enmarcaremos el levantamiento del plan de seguridad en la metodología Magerit y aplicaremos la metodología OSSTMM como instrumento de testeo de la eficacia del plan de seguridad. Para ello debemos cumplir las siguientes tareas:

- Recopilación de información.
- Desarrollo del plan de seguridad.
- Test de eficacia del plan de seguridad.

4.1. Recopilación de información

Según la metodología Magerit el desarrollo de un plan de seguridad informática parte del análisis de riesgos a los que está sujeto el sistema de información. Para aquello la misma metodología presenta un método de análisis de riesgos que sigue una aproximación metódica para determinar el riesgo.

Para llevar a fin el análisis de riesgos debemos completar las siguientes tareas:

- Caracterización de los activos.
- Caracterización de las amenazas.
- Determinación del riesgo potencial.
- Caracterización de las salvaguardas.

4.1.1. Caracterización de los activos

La caracterización de los activos busca conocer los aspectos más relevantes y necesarios para poder llevar a cabo el análisis de riesgos, como nos indica la metodología Magerit, nos interesa conocer el tipo de activos que maneja el sistema sujeto de estudio, las dependencias que existe entre dichos activos y el valor que tiene cada uno de los activos (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012k).

Las subtareas que debemos realizar para completar la tarea son las siguientes:

- Identificación de los activos.
- Dependencias entre activos.

- Valoración de los activos.

4.1.1.1. Identificación de los activos

Con la ayuda del marco que proporciona la metodología Magerit, dividimos los activos en dos grupos definidos, los activos esenciales y los activos de los cuales el sistema depende para aprovisionar el servicio.

Activos esenciales: En el sistema sujeto de estudio se identificaron dos activos esenciales:

- La información que se maneja.
- Los servicios que se presta.

Dado que nuestro estudio se enfocó en riesgos de Ataque de Hombre en el Medio y se conoce que dicho ataque es usado para robo o manipulación de la información que circula en un sistema (Conti et al., 2014d) el activo información tendrá mayor relevancia y marcará los requisitos de seguridad del sistema (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012q).

Por lo dicho los activos esenciales identificados son los siguientes:

- **info-per:** Información personal.
- **services-int-pub:** Servicio de internet de carácter público sin relación contractual.

Activos de los que depende el servicio: El servicio que provee el sistema definirá los activos necesarios para el aprovisionamiento de dicho servicio entre ellos encontraremos el equipo hardware, el software servicios de conectividad, entre otros.

Los activos Hardware identificados en el escenario de estudio son los siguientes:

- **hw-network-wap:** Equipamiento de soporte de red punto de acceso inalámbrico.

Los activos Software identificados en el escenario de estudio son los siguientes:

- **sw-network-wap:** Firmware del equipo de soporte de red inalámbrico.

El activo de redes de comunicaciones que se ha identificado en el escenario de estudio es el siguiente:

- **con-internet-ser:** Conectividad al internet como servicio.
- **con-internet-ext:** Conectividad al internet contratada a un tercero.

En este epílogo aparecen las personas relacionadas con el sistema de información:

- **per-user:** Usuario final o beneficiario del servicio.
- **per-admin:** Administrados de la infraestructura que ofrece el servicio.

4.1.1.2. Dependencias entre activos

Magerit define a las dependencias entre activos como el grado en el cual un activo se ve afectado por una amenaza materializada en un activo del cual depende (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012r).

Una vez identificados los activos de nuestro escenario de estudio lo siguiente que nos corresponde es realizar un árbol de dependencias. En nuestro caso la dependencia entre activos es directa con el servicio que manejan la información, a su vez el activo servicio de conectividad a internet depende directamente y en igual magnitud de sus activos hijos. Las personas que administran y usan el servicio son transversales al sistema ya que el sistema no almacena información y los propietarios de esta son las mismas personas (Figura 1-4).

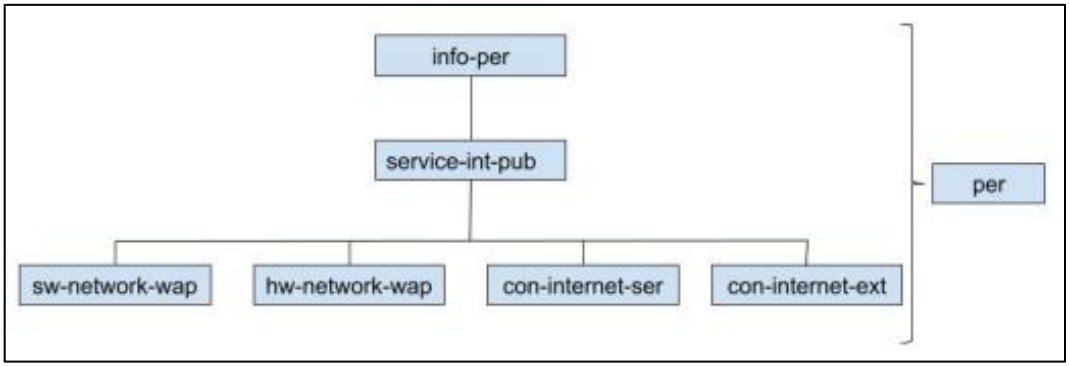

Figura 1-4: Dependencias entre activos

Realizado por: Fiallos, Ricardo, 2022.

4.1.1.3. Valoración de los activos

Los activos importan por lo que valen para la organización o representan para sus propietarios, como ya hemos mencionado nuestro interés de estudio se centra en el caso de materialización de amenazas de ataque de Hombre en el medio, por lo que el valor se centra en el activo información

personal, para poder definir el valor de este activo, nos referiremos a la encuesta TIC 2017 realizada y publicada por el INEC.

Para determinar el valor de la Información Personal que fluye por las redes de acceso público, dividiremos este activo en tres activos:

- Información personal de nivel alto.
- Información personal de nivel medio.
- Información personal de nivel bajo.

Usaremos los datos de la encuesta TICs 2017 efectuada por el INEC a nivel nacional para caracterizar el porcentaje de cada tipo de información. Para ello filtraremos la encuesta por edad (16 a 40 años de edad) de los encuestados y las personas que usaron centros de acceso público para conectarse al Internet.

De este grupo de personas nos interesa conocer el tipo de uso de que le dan al internet, datos que se visualizan en la Tabla 1-4:

Tabla 1-4: Uso de Internet Encuesta TICs 2017 INEC

Uso	Porcentaje
Obtener información	34.0
Comunicación en general	42.4
Comprar / ordenar productos o servicios	0.6
Banca electrónica y serv. financieros	0.4
Educación y aprendizaje	17.0
Transacciones con organismos	0.1
Actividades de entretenimiento	3.0
Obtener películas, música o software	0.9
Leer descargar libros electrónicos	0.3
Razones de trabajo	1.5
TOTAL	100.0

Realizado por: Fiallos, Ricardo, 2022.

Con los datos proporcionados por el INEC, caracterizaremos el porcentaje de cada tipo de información basados en las tablas que provee la guía Magerit (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012s).

Tabla 2-4: Valor del activo Información Personal

Uso	Porcentaje	[D]	[I]	[C]	[A]	[T]

Obtener información	34.0	-	2	3	3	1
Comunicación en general	42.4	-	3	5	3	1
Comprar / ordenar productos o servicios	0.6	-	3	3	5	3
Banca electrónica y serv. financieros	0.4	-	5	6	6	4
Educación y aprendizaje	17.0	-	3	3	3	1
Transacciones con organismos	0.1	-	5	6	6	4
Actividades de entretenimiento	3.0	-	1	2	2	1
Obtener películas, música o software	0.9	-	1	3	2	1
Leer descargar libros electrónicos	0.3	-	1	3	2	1
Razones de trabajo	1.5	-	5	6	4	2
VALOR	-	-	2.62	3.88	3.00	1.04

Realizado por: Fiallos, Ricardo, 2022.

Dado que la información personal fluye en el servicio y este depende directamente de sus activos hijos la dependencia de todos los activos es directa, por lo que los activos hijos heredaran la totalidad del valor del activo esencial Información personal. El apéndice Fichas de Activos muestra el detalle de lo mencionado. La Tabla 3-4 muestra en resumen el valor de los activos.

Tabla 3-4: Valor de los activos

	Dimensiones				
Activos	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Información personal	[2.62]	[3.88]	[3.00]	[1.04]	
Servicio de internet de carácter público	[5.00]	[2.62]	[3.88]	[8.00]	[5.04]
Punto de acceso inalámbrico	[5.00]	[2.62]	[3.88]	[8.00]	[1.04]
Firmware del punto de acceso inalámbrico	[5.00]	[2.62]	[3.88]	[8.00]	[1.04]
Conexión a internet proporcionada por un tercero	[5.00]	[2.62]	[3.88]	[8.00]	[1.04]
Conexión a internet proporcionada por la entidad	[5.00]	[2.62]	[3.88]	[8.00]	[1.04]

Realizado por: Fiallos, Ricardo, 2022.

4.1.2. Caracterización de las amenazas

Esta actividad consta de dos sub-tareas:

- Identificación de las amenazas.
- Valoración de las amenazas.

4.1.2.1. Identificación de las amenazas

Continuando con el uso de la metodología Magerit identificaremos las amenazas que correspondan a los activos tomando en cuenta que nuestro foco de estudio es la posible materialización de amenazas de ataques de hombre en el medio en entornos de red IEEE 802.11b/g/n de acceso libre. Por ello el estudio de las amenazas se centrará en el activo Servicio de internet de carácter público sin relación contractual (services-int-pub) y sus activos hijos ya que en éstos se genera la comunicación entre el usuario del servicio por tanto la Conectividad al Internet de manera inalámbrica siendo estos el objetivo de posibles ataques de Hombre en el Medio, dando como resultado en su materialización degradación de seguridad del activo Información Personal (info-per).

El activo Conectividad al internet contratado a un tercero (con-internet-ext) es un activo hijo de Servicio de internet de carácter público sin relación contractual (services-int-pub) pero al ser un servicio provisto por un tercero trasladaremos sus riesgos a la entidad que provee el servicio.

También consideramos que, no todas las amenazas listadas en la metodología Magerit conllevan un riesgo de Ataque he Hombre en el Medio por lo que el presente estudio se centrará también en aquellas amenazas que se liguen a los ataques foco de estudio.

Luego de tomar los criterios de exclusión mencionados las amenazas localizadas se resumen en la siguiente Tabla 4-4:

Tabla 4-4: Identificación de las amenazas

Activos	Amenazas
sw-network-wap	E.21 Errores de mantenimiento / actualización de programas (software)
	A.8 Difusión de software dañino
	A.22 Manipulación de programas
hw-network-wap	E.2 Errores del administrador
	E.23 Errores de mantenimiento / actualización de equipos (hardware)
	E.24 Caída del sistema por agotamiento de recursos
	E.25 Pérdida de equipos
	A.6 Abuso de privilegio de acceso
	A.11 Acceso no autorizado
con-internet-ser	A.5 Suplantación de la identidad del usuario
	A.9 Re-encaminamiento de mensajes
	A.12 Análisis de tráfico

	A.15 Modificación deliberada de la información
	A.24 Denegación de servicios

Realizado por: Fiallos, Ricardo, 2022.

4.1.2.2. Valoración de las amenazas

Una vez localizadas las amenazas que pueden afectar a cada activo lo siguiente será determinar la degradación que provocaría la materialización de dicha amenaza en cada dimensión de seguridad de cada activo. La escala usada se muestra en la Tabla 5-4.

Tabla 5-4: Degradación del valor

Degradación	[A]Alta
	[M]Media
	[B]Baja

Realizado por: Fiallos, Ricardo, 2022.

Por otro lado, también se debe determinar la probabilidad de ocurrencia de la materialización de dicha amenaza.

Para esta tarea la guía Magerit recomienda usar datos históricos de ocurrencia. Al no existir una regulación en el país que proteja la información personal no contamos con datos históricos de ocurrencia de degradación de la seguridad de este activo, por lo que realizamos una encuesta a profesionales del área de Seguridad Informática para obtener los valores de ocurrencia de materialización de las amenazas. La valoración de las amenazas se muestra en la Tabla 6-4.

Tabla 6-4: Valoración de las amenazas

Activos	Amenazas	[P]	[D]	[I]	[C]	[A]	[T]
sw-net-wap	E.21 Errores de mantenimiento / actualización de programas (software)	A	A	A			
	A.8 Difusión de software dañino	A	A	A	M		
	A.22 Manipulación de programas	A	A	A	M		
hw-net-wap	E.2 Errores del administrador	M	M	M	B		
	E.23 Errores de mantenimiento / actualización de equipos (hardware)	A	A				
	E.24 Caída del sistema por agotamiento de recursos	M	A				
	E.25 Perdida de equipo	M	A				
	A.6 Abuso de privilegio de acceso	A	A	A	M		
	A.11 Acceso no autorizado	M		M	M		
con-inter-ser	A.5 Suplantación de la identidad del usuario	A		A	A	A	
	A.9 Re-encaminamiento de los mensajes	A			A		
	A.12 Análisis de trafico	A			M		
	A.15 Modificación deliberada de la información	A		A			
	A.24 Denegación de servicios	A	A				

Realizado por: Fiallos, Ricardo, 2022.

4.1.3. Determinación del riesgo potencial

Dado que el escenario en el que desarrollamos nuestro análisis es de estudio procederemos a obtener el riesgo potencial, para ello seguiremos los siguientes pasos:

- Determinación del impacto potencial.
- Determinación del riesgo potencial.

4.1.3.1. Determinación del impacto potencial

El impacto potencial es el daño que sufre un activo tras la materialización de una amenaza en cada una de las dimensiones de seguridad. Para determinar el impacto que sufre el activo tras esta materialización se debe conocer el valor del activo en cada dimensión de seguridad y la degradación que causan las amenazas.
Para el cumplimiento de esta actividad usaremos la Tabla 7-4 (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012t) y la Tabla 8-4 (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012u).

Tabla 7-4: Valor de los activos

Valor		**Criterio**
10	[E] extremo	daño extremadamente grave
9	[MA] muy alto	daño muy grave
6-8	[A] alto	daño grave
3-5	[M] medio	daño importante
1-2	[B] bajo	daño menor
0	[MB] despreciable	irrelevante a efectos prácticos

Realizado por: Fiallos, Ricardo, 2022.

Tabla 8-4: Impacto

		Degradación		
		B	**M**	**A**
Valor	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Realizado por: Fiallos, Ricardo, 2022.

Tabla 9-4: Impacto potencial de las amenazas sobre los activos

Activos	Amenazas	Degradación					Valor					Impacto				
		[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
sw-net-wap	E.21 Errores de mantenimiento / actualización de programas (software)	A	A				M	B	M	A	B	B				
	A.8 Difusión de software dañino	A	A	M			M	B	M	A	B	B	B			
	A.22 Manipulación de programas	A	A	M			M	B	M	A	B	B	B			
hw-net-wap	E.2 Errores del administrador	M	M	B			M	B	M	A	B	MB	MB			
	E.23 Errores de mantenimiento / actualización de equipos (hardware)	A					M	B	M	A	B	M				
	E.24 Caída del sistema por agotamiento de recursos	A					M	B	M	A	B	M				
	E.25 Perdida de equipo	A					M	B	M	A	B	M				
	A.6 Abuso de privilegio de acceso	A	A	M			M	B	M	A	B	M	B	B		
	A.11 Acceso no autorizado		M	M			M	B	M	A	B		MB	B		
con-inter-ser	A.5 Suplantación de la identidad del usuario		A	A	A		M	B	M	A	B		B	M	A	
	A.9 Re-encaminamiento de los mensajes			A			M	B	M	A	B			M		
	A.12 Análisis de trafico			M			M	B	M	A	B			B		
	A.15 Modificación deliberada de la información		A				M	B	M	A	B		B			
	A.24 Denegación de servicios	A					M	B	M	A	B	M				

Realizado por: Fiallos, Ricardo, 2022.

4.1.3.2. Determinación del riesgo potencial

El riesgo potencial es la medida del daño que podría sufrir un activo tras la materialización de una amenaza. Para conocer el riesgo se debe conocer antes el impacto, conocido solo queda derivar el riesgo de la probabilidad materialización de la amenaza.

Para derivar el riesgo del impacto por medio de la probabilidad usaremos la Tabla 10-4 (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012l) y la Tabla 11-4 muestra los resultados obtenidos al conocer el riesgo tras la derivación del impacto con la probabilidad (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012m).

Tabla 10-4: Riesgo

		Probabilidad		
		B	**M**	**A**
Impacto	**A**	A	A	MA
	M	M	M	A
	B	B	B	M

Realizado por: Fiallos, Ricardo, 2022.

Tabla 11-4: Riesgo potencial de las amenazas sobre los activos

Activos	Amenazas	Impacto						Riesgo				
		[D]	[I]	[C]	[A]	[T]	[P]	[D]	[I]	[C]	[A]	[T]
sw-net-wap	E.21 Errores de mantenimiento / actualización de programas (software)	M	B				A	A	M			
	A.8 Difusión de software dañino	M	B	B			A	A	M	M		
	A.22 Manipulación de programas	M	B	B			A	A	M	M		
hw-net-wap	E.2 Errores del administrador	B	MB	MB			M	B	MB	MB		
	E.23 Errores de mantenimiento / actualización de equipos (hardware)	M					A	A				
	E.24 Caída del sistema por agotamiento de recursos	M					M	M				
	E.25 Perdida de equipo	M					M	M				
	A.6 Abuso de privilegio de acceso	M	B	B			A	A	M	M		
	A.11 Acceso no autorizado		MB	B			M		MB	B		
con-inter-ser	A.5 Suplantación de la identidad del usuario		B	M	A		A		M	A	MA	
	A.9 Re-encaminamiento de los mensajes			M			A			A		
	A.12 Análisis de trafico			B			A			M		
	A.15 Modificación deliberada de la información		B				A		M			
	A.24 Denegación de servicios	M					A	A				

Realizado por: Fiallos, Ricardo, 2022.

4.1.4. Caracterización de las salvaguardas

Las salvaguardas son procedimientos o mecanismos tecnológicos que buscan reducir el riesgo (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012n).

Para el estudio inicial del riesgo potencial consideramos un sistema sin salvaguardas. lo siguiente que nos corresponde es determinar las salvaguardas a implementar según los activos y amenazas caracterizadas anteriormente. Para ello usaremos las salvaguardas por cada tipo de activo que presenta Magerit (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012o).

De esta lista, escogeremos las salvaguardas que apliquen y se justifiquen para reducir los riesgos localizados. La Tabla 12-4 muestra las salvaguardas escogidas para cada activo.

Tabla 12-4: Salvaguardas por cada activo

Activos	Salvaguardas
Todos los activos	H.tools.VA Herramienta de análisis de vulnerabilidades
	H.tools.TM Herramienta de motorización de trafico
Software del AP	SW.CM Cambios (actualizaciones y mantenimiento)
	SW.SC Se aplican perfiles de seguridad
Hardware del AP	HW.A Aseguramiento de la disponibilidad
	HW.CM Cambios (actualizaciones y mantenimiento)
Comunicación WiFi	COM.I Protección de la integridad de los datos intercambiados
	COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
	COM.internet Internet: uso de ? acceso a?
	COM.wifi Seguridad Wireless (WiFi)

Realizado por: Fiallos, Ricardo, 2022.

Las salvaguardas listadas anteriormente tendrán una eficacia porcentual de acuerdo a su nivel de madures e idoneidad para el tratamiento del riesgo, un Plan de Seguridad Informática está sujeto a la revisión y mejora continua, en el presente trabajo de investigación valoraremos la eficacia de las salvaguardas según el criterio tomado de (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012o) que se muestra en la Tabla 13-4.

Tabla 13-4: Eficacia y madures de las salvaguardas

Factor	Nivel	Significado
0	L0	Inexistente
0.2	L1	Inicial
0.4	L2	Reproducible, pero intuitivo
0.6	L3	Proceso definido
0.8	L4	Gestionado y medible
1	L5	Optimizado

Realizado por: Fiallos, Ricardo, 2022.

4.2. Test de eficacia del plan de seguridad

Testear la seguridad de un sistema conlleva varias tareas que se deben organizar adecuadamente con la finalidad de no olvidar ninguna de ellas en el proceso. Para esto definir la prueba de seguridad es el primer paso a realizar (ISECOM, 2010e).

4.2.1. Definición de la prueba de seguridad

Siguiendo la guía OSSTMM V3 se define la prueba de seguridad en 7 pasos:

4.2.1.1. ¿Qué deseamos proteger?

El activo de información foco de protección es la información personal del usuario, dicha información transita a través del servicio hacia el internet. Este activo marcará las necesidades de seguridad del sistema.

4.2.1.2. Zona de enfrentamiento

La zona de enfrentamiento del activo de información a proteger es la comunicación inalámbrica del estándar IEEE 802.11 b/g/n.

4.2.1.3. Alcance

Este parámetro indica todo lo que está fuera de la Zona de enfrentamiento que es necesario para la provisión del servicio, en nuestro caso:

- Equipos.
- Hardware.
- Software.

- Conectividad.
- Servicio de conectividad al internet.
- Protocolos.
- Energía eléctrica.
- Usuarios.

4.2.1.4. Vectores

Conexión al servicio: El usuario negocia el ingreso a la red de acuerdo a los parámetros de control de acceso establecidos, una vez aprobado el ingreso el usuario recibe los permisos correspondientes.

Uso del servicio: El usuario tiene acceso a los recursos que el sistema provee dentro de parámetros de tiempo, cantidad y uso adecuado previamente establecidos.

Desconexión: Trascurrido el tiempo establecido para el uso de los recursos del servicio el sistema desconecta al usuario, o el usuario tras completar la necesidad de uso de los recursos cierra la conexión al sistema.

4.2.1.5. Equipos necesarios para la prueba

Los equipos necesarios son los siguientes:

- Computador con tarjeta inalámbrica
- Sistema Operativo Kali linux
- Herramienta de revisión de vulnerabilidades
- Herramientas de pruebas de penetración.

La interacción que será objeto del presente estudio se presenta en el canal inalámbrico.

4.2.1.6. Tipo de prueba

La prueba que se realizará es de auditoría interna o caja transparente, ya que conocemos a detalle los controles y pormenores del sistema. Esta prueba nos permite conocer la efectividad de los controles dispuestos.

4.2.1.7. Marco legal

Dado que las pruebas de penetración se darán en un escenario de pruebas controlado no se incurre en ningún tipo de acción que conlleve a futuras responsabilidades legales.

En el caso de realizar esta prueba en ambientes en producción se deberá contar con la debida autorización de la entidad que provee el servicio y asegurar las medidas necesarias que garanticen los parámetros de regulación legal establecidos a la fecha del testeo.

4.2.2. Cálculo del RAV

El RAV es el cálculo del balance que existe entre la porosidad, los controles y las limitantes. Este balance puede determinar si los controles que se realizan en el sistema son insuficientes, suficientes o excesivos (ISECOM, 2010e).

Para el cálculo la ISECOM pone a disposición en su web oficial https://www.isecom.org/ una hoja de cálculo que facilita la obtención de los valores necesarios para caracterizar el balance en la seguridad del sistema.

El cálculo del RAV se realiza sobre cada canal de la zona de enfrentamiento definida. Para obtener el valor RAV se han clasificado los valores necesarios en los siguientes conjuntos (ISECOM, 2010f):

- Porosidad u Op-Sec.
- Controles de interacción o Clase A.
- Controles de proceso o Clase B.
- Limitaciones.

4.2.3. Cálculo del RAVS en escenario sin aplicar el plan de seguridad

Dado que, resulta sumamente complejo generalizar el estado actual de todas las redes de acceso libre del estándar IEEE 802.11b/g/n se asumirá el estado inicial de la red (sin aplicar el plan de seguridad) una red con controles inexistentes.

El diagrama del escenario se muestra en la Ilustración 2-4.

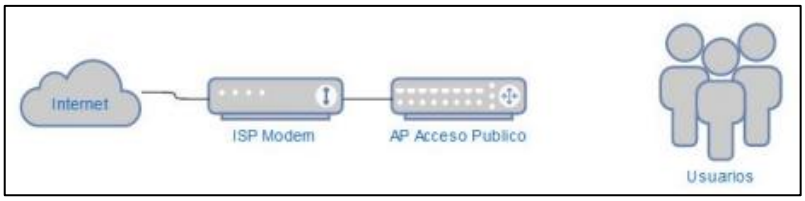

Figura 2-4: Diagrama infraestructura inicial

Realizado por: Fiallos, Ricardo, 2022.

4.2.3.1. Porosidad u Op-Sec en escenario inicial

Tabla 14-4: Porosidad para el cálculo de RAV - Escenario inicial

Porosidad			
Ítem	**Prueba**	**Herramienta**	**Cant.**
Visibilidad	Servicios visibles	Nmap	1
	Señal fuera de rango establecido	Antena	1
	Fuentes que interactúan sin autorización	Wireshark	0
Acceso	Acceso al servicio sin horario	Computador	1
	Acceso al servicio en lugares no dispuestos	Antena	1
	AP con configuraciones de fabrica	Nessus	0
	Controles de acceso pobres o inexistentes	Aircrack	1
Confianza	Autenticación normal del cliente	Computador	1
	Autenticación con credenciales falsas	Aircrack	1
	Traspaso de credenciales a terceros	Computador	1
TOTAL			8

Realizado por: Fiallos, Ricardo, 2022.

4.2.3.2. Controles de interacción o Clase A en escenario inicial

Tabla 15-4: Controles de interacción o Clase A - Escenario inicial

Controles de interacción o Clase A			
Ítem	**Prueba**	**Herramienta**	**Cant.**
Autenticación	Contraseña de acceso	Punto de acceso	1
	Usuario y contraseña	Portal cautivo	0
	Acceso por dirección física	Portal cautivo	0
	Un dispositivo por usuario	Portal cautivo	0

	Horario de uso	Portal cautivo	0
	Tiempo de uso	Portal cautivo	0
Indemnización	Términos de uso del servicio	Portal cautivo	0
Elasticidad	Negar servicio en caso de fallas	IPS	0
Subyugación	Autenticación cifrada	Llave SSL	0
Continuidad	Suministro eléctrico	UPS	0
	Enlace redundare	ISP adicional	0
	Balanceo	Enrutador	0
TOTAL			1

Realizado por: Fiallos, Ricardo, 2022.

4.2.3.3. Controles de proceso o Clase B en escenario inicial

Tabla 16-4: Controles de proceso o Clase B - Escenario inicial

Controles de proceso o Clase B			
Ítem	**Prueba**	**Herramienta**	**Cant.**
No-Repudio	Logs de acceso al servicio	Portal cautivo	0
	Llave SSL para autenticar ingreso	Portal cautivo	0
Confidencialidad	Perfil del administrador del sistema	Equipos	0
	Negar configuración por red WIFI	Equipos	0
	Contraseña robusta	Equipos	0
Privacidad	Lista negra de páginas maliciosas	Cortafuegos	0
	Uso exclusivo de tráfico cifrado	Cortafuegos	0
Integridad	Uso exclusivo de tráfico cifrado	Cortafuegos	0
Alarma	Agotamiento de recursos	Punto de acceso	0
	Detección de intrusos	IDS	0
TOTAL			0

Realizado por: Fiallos, Ricardo, 2022.

4.2.3.4. Limitaciones en escenario inicial

Tabla 17-4: Limitaciones - Escenario inicial

Limitaciones			
Ítem	**Prueba**	**Herramienta**	**Cant.**
Vulnerabilidad	Niega el acceso para usuarios autorizados	Metasploit	1
	Permite el acceso para usuarios no autorizados	Metasploit	1
	Permite a usuarios que se oculten del alcance	Metasploit	0
Debilidad	Ingreso al sistema por fuerza bruta	Hydra	0

	Descifrar contraseñas por diccionario	Crunch	1
	Clonar direcciones físicas	Macchanger	1
Preocupación	Escalamiento de privilegios	Nessus, Metasploit	0
Exposición	Escaneo de direcciones IP	Nmap	1
	Escaneo de puertos	Nmap	1
Anomalías		IDS	0
TOTAL			6

Realizado por: Fiallos, Ricardo, 2022.

4.2.3.5. Cálculo de RAVS para escenario inicial

Una vez culminado el análisis del sistema procederemos a ingresar los valores en la hoja de cálculo proporcionada por la ISECOM en su página oficial:

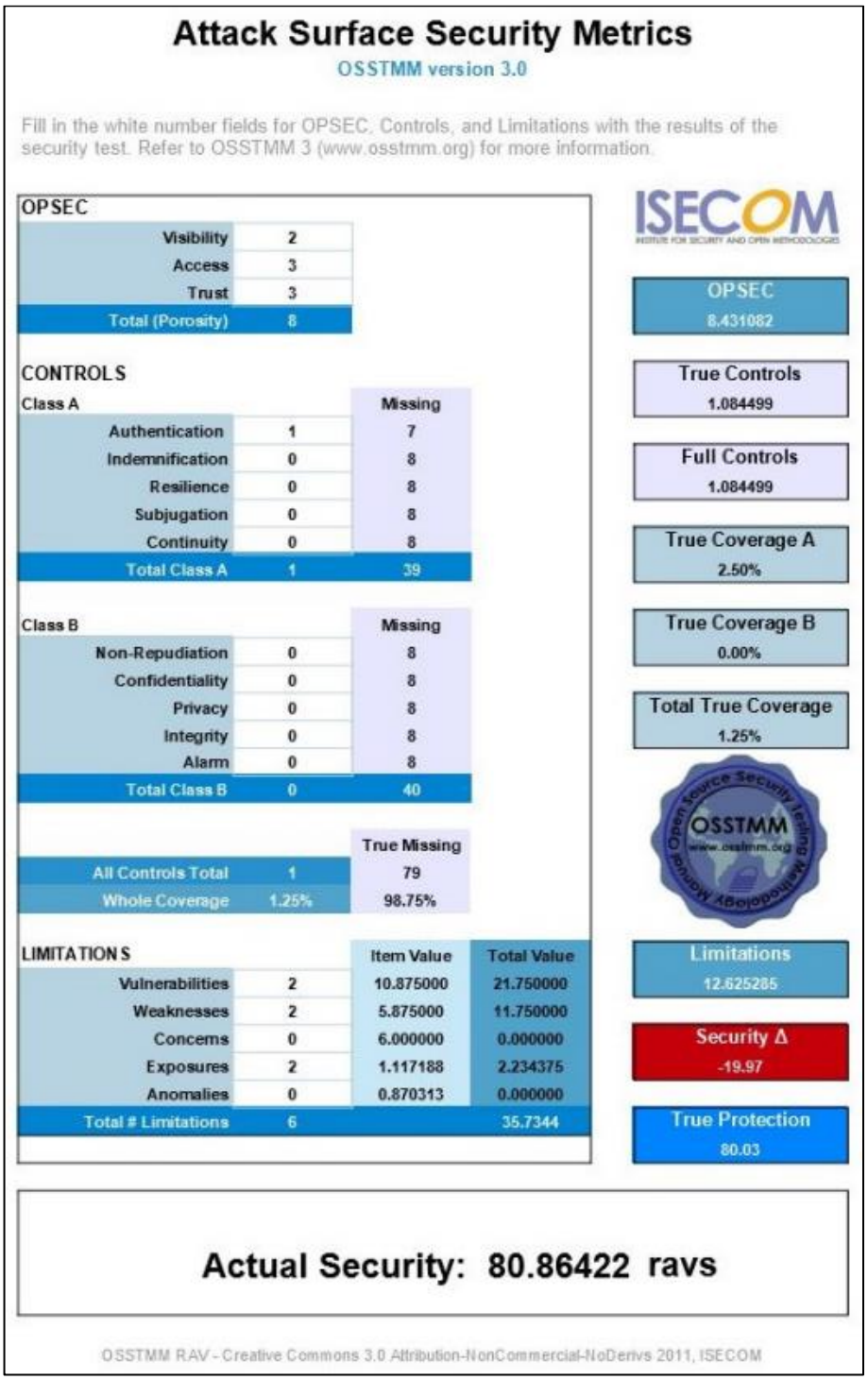

Figura 3-4: Cálculo de RAVS - Escenario inicial

Fuente: ISECOM, 2010a, p. 80.

Realizado por: Fiallos, Ricardo, 2022.

4.2.4. Cálculo del RAVS en escenario con el plan de seguridad aplicado

Una vez aplicado el plan de seguridad al sistema la infraestructura instalada se muestra en la Ilustración 4-4.

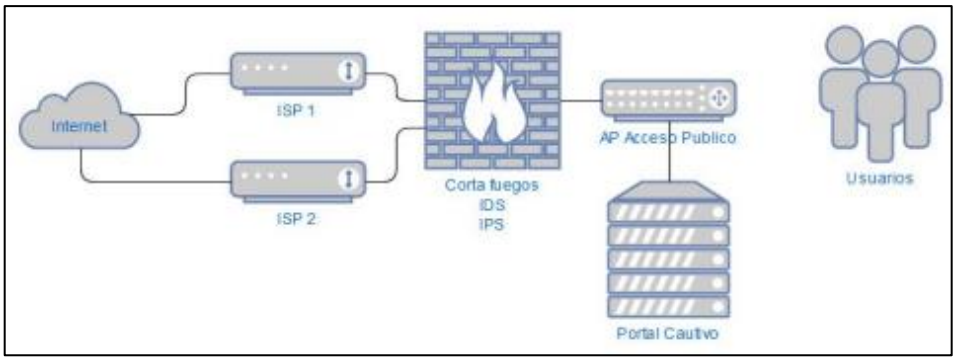

Figura 4-4: Diagrama infraestructura con el plan de seguridad aplicado

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.1. Porosidad u Op-Sec en escenario con el plan de seguridad aplicado

Tabla 18-4: Porosidad para el cálculo de RAV - Escenario con el plan de seguridad aplicado

Porosidad			
Ítem	**Prueba**	**Herramienta**	**Cant.**
Visibilidad	Servicios visibles	Nmap	1
	Señal fuera de rango establecido	Antena	0
	Fuentes que interactúan sin autorización	Wireshark	0
Acceso	Acceso al servicio sin horario	Computador	0
	Acceso al servicio en lugares no dispuestos	Antena	0
	AP con configuraciones de fábrica	Nessus	0
	Controles de acceso pobres o inexistentes	Aircrack	0
Confianza	Autenticación normal del cliente	Computador	1
	Autenticación con credenciales falsas	Aircrack	0
	Traspaso de credenciales a terceros	Computador	0
TOTAL			2

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.2. Controles de interacción o Clase A en escenario con el plan de seguridad aplicado

Tabla 19-4: Controles de interacción o Clase A - Escenario con el plan de seguridad aplicado

Controles de interacción o Clase A			
Ítem	**Prueba**	**Herramienta**	**Cant.**
Autenticación	Contraseña de acceso	Punto de acceso	0
	Usuario y contraseña	Portal cautivo	1
	Acceso por dirección física	Portal cautivo	0
	Un dispositivo por usuario	Portal cautivo	1
	Horario de uso	Portal cautivo	1
	Tiempo de uso	Portal cautivo	1
Indemnización	Términos de uso del servicio	Portal cautivo	1
Elasticidad	Negar servicio en caso de fallas	IPS	1
Subyugación	Autenticación cifrada	Llave SSL	1
Continuidad	Suministro eléctrico	UPS	1
	Enlace redundare	ISP adicional	1
	Balanceo	Enrutador	1
TOTAL			10

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.3. Controles de proceso o Clase B en escenario con el plan de seguridad aplicado

Tabla 20-4: Controles de proceso o Clase B - Escenario con el plan de seguridad aplicado

Controles de proceso o Clase B			
Ítem	**Prueba**	**Herramienta**	**Cant.**
No-Repudio	Logs de acceso al servicio	Portal cautivo	1
	Llave SSL para autenticar ingreso	Portal cautivo	1
Confidencialidad	Perfil del administrador del sistema	Equipos	1
	Negar configuración por red	WIFI Equipos	1
	Contraseña robusta	Equipos	1
Privacidad	Lista negra de páginas maliciosas	Cortafuegos	1
	Uso exclusivo de tráfico cifrado	Cortafuegos	1
Integridad	Uso exclusivo de tráfico cifrado	Cortafuegos	1
Alarma	Agotamiento de recursos	Punto de acceso	0
	Detección de intrusos	IDS	1
TOTAL			9

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.4. Limitaciones en escenario con el plan de seguridad aplicado

Tabla 21-4: Limitaciones - Escenario con el plan de seguridad aplicado

Limitaciones			
Ítem	**Prueba**	**Herramienta**	**Cant.**
Vulnerabilidad	Niega el acceso para usuarios autorizados	Metasploit	1
	Permite el acceso para usuarios no autorizados	Metasploit	0
	Permite a usuarios que se oculten del alcance	Metasploit	0
Debilidad	Ingreso al sistema por fuerza bruta	Hydra	0
	Descifrar contraseñas por diccionario	Crunch	0
	Clonar direcciones físicas	Macchanger	1
Preocupación	Escalamiento de privilegios	Nessus, Metasploit	0
Exposición	Escaneo de direcciones IP	Nmap	1
	Escaneo de puertos	Nmap	1
Anomalías		IDS	0
TOTAL			4

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.5. Cálculo de RAVS para escenario con el plan de seguridad aplicado

Para realizar el cálculo de los RAVS deberemos repetir el llenado de la matriz con los criterios del cálculo de la porosidad, cálculo de los controles y las limitaciones.

4.2.4.6. Cálculo de la porosidad

Para conocer el cálculo de la porosidad se deben conocer los valores de la Visibilidad, Acceso y Confianza, en la Ilustración siguiente se muestran los criterios a usar para la obtención de estos valores.

Figura 5-4: Cálculo de RAVS - Escenario con el plan de seguridad aplicado

Fuente: ISECOM, 2010a, p. 80.

Realizado por: Fiallos, Ricardo, 2022.

Tabla 22-4: Porosidad para el cálculo de RAV

Porosidad		
Ítem	**Prueba**	**Total**
Visibilidad	Número de usuarios conectados al servicio al momento de la prueba	0
Acceso	Corresponde al número de accesos no autorizados que puede darse en el sistema	0
Confianza	Cantidad de servicios a los que accede el usuario al ingresar al sistema	0

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.7. Cálculo de los controles

Son los mecanismos de seguridad dispuestos en el sistema para protegerlo. El resumen de los criterios de cálculo se presenta en la Tabla 36-4.

Tabla 23-4: Controles Clase A - Cálculo de RAV

Controles de interacción o clase A		
Ítem	**Prueba**	**Total**
Autenticación	Cada proceso de autenticación necesario para obtener acceso al servicio	0
Indemnización	Legalidad del uso del servicio	0
Elasticidad	Controles que nieguen el servicio en caso de fallas de seguridad	0
Subyugación	Permite acceder al sistema sin necesidad credenciales con distintos atributos	0
Continuidad	Controles dispuestos para mantener activo el servicio en caso de fallos	0

Realizado por: Fiallos, Ricardo, 2022.

Tabla 24-4: Controles Clase B - Cálculo de RAV

Controles de interacción o clase B		
Ítem	**Prueba**	**Total**
No-Repudio	Controles que garanticen el proceso de autenticación	0
Confidencialidad	Controles que garanticen la confidencialidad de los datos transmitidos	0
Privacidad	Controles que garanticen la privacidad de los datos transmitidos	0
Integridad	Controles que garanticen la integridad de los datos transmitidos	0
Alarma	Alertas programadas ante posibles ataques o fallas	0

Realizado por: Fiallos, Ricardo, 2022.

4.2.4.8. Limitaciones

Tabla 25-4: Limitaciones - Cálculo de RAV

Limitaciones		
Ítem	**Prueba**	**Total**
Vulnerabilidad	Vulnerabilidades encontradas en el sistema que puedan conllevar a la materialización de ataque de hombre en el medio. Se obtiene este valor a través de un escaneo de vulnerabilidades o prueba de penetración.	0
Debilidad	Debilidades conocidas, detectadas o escaneadas de los controles. Un ejemplo de esto sería el caso de que no se controle la cantidad de intentos fallidos a poner la clave de ingreso al sistema, lo que ocasionaría la posibilidad de ingreso al sistema por fuerza bruta.	0
Preocupación	Banderas o errores que por su condición podrían generar problemas en la ejecución de los procesos de control. Como ejemplo citaremos a una mala configuración del almacenamiento de los logs del sistema.	0
Exposición	Cuente cada acción, falla o error injustificable que proporcione visibilidad indirecta de objetivos o activos dentro del canal de alcance elegido.	0
Anomalías	Cuente cada elemento no identificable o desconocido que no puede ser contabilizado en operaciones normales. Alertas de seguridad tempranas.	0

Realizado por: Fiallos, Ricardo, 2022.

4.3. Valoración de Resultados

Una vez concluido el desarrollo del plan de seguridad, lo siguiente será analizar los resultados del mismo al momento de enfrentar al sistema a ataques de Hombre en el medio. Para ello analizaremos los factores que influirán el ataque en los dos escenarios.

4.3.1. Criterios de valoración

Como podemos observar en el Capítulo 3, la metodología Magerit enmarca su desarrollo en amenazas generales que al cubrirlas el sistema reduce los riesgos.

Por lo que se procederá a valorar el nivel de reducción de los riesgos puntualmente de ataques de hombre en el medio en entornos de red del estándar IEEE 802.11b/g/n tras la aplicación del plan

de seguridad con los criterios de valoración de riesgo de materialización de amenazas enmarcado en la metodología Magerit, incorporando a este análisis la matriz Probabilidad de ocurrencia Tabla 39-4 (Plosz et al., 2016f), para la obtención del valor de la probabilidad de ataque.

Tabla 26-4: Probabilidad de ocurrencia

Motivación\Dificultad	**Baja**	**Media**	**Alta**
Baja	[PP] Poco probable		
Media	[MP] Muy probable	[P] Probable	[PP] Poco probable
Alta	[MP] Muy probable	[MP] Muy probable	[PP] Poco probable

Realizado por: Fiallos, Ricardo, 2022.

Para determinar el impacto usaremos la matriz Impacto Tabla 40-4, donde el valor del activo se tomará el valor del activo de información; Información personal de la Tabla 8-4.

Tabla 27-4: Impacto

		Degradación		
		B	**M**	**A**
Valor	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Realizado por: Fiallos, Ricardo, 2022.

Con los valores del impacto y la probabilidad obtendremos el valor de Riesgo usando los criterios de la matriz Riesgo Tabla 41-4. Esto lo realizaremos tanto para el escenario sin plan de seguridad como para el escenario con plan de seguridad aplicado, obteniendo así los valores de riesgo potencial y residual para ataques de hombre en el medio.

Tabla 28-4: Riesgo

		Probabilidad		
		B	**M**	**A**
Impacto	**A**	A	A	MA
	M	M	M	A
	B	B	B	M

Realizado por: Fiallos, Ricardo, 2022.

4.3.2. Valoración de los riesgos sin plan de seguridad

Empezaremos por valorar los riesgos mencionados en el escenario sin plan de seguridad.

Tabla 29-4: Impacto de las amenazas de ataque de hombre en el medio - Sin plan de seguridad

	Amenazas	**Degradación**					**Valor**					**Impacto**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Ataques MiM	ARP Spoofing	B	M	A	B	B	M	B	M	A	B	MB	MB	M	B	MB
	DNS Spoofing	B	M	A	B	B	M	B	M	A	B	MB	MB	M	B	MB
	DHCP Spoofing	B	M	A	B	B	M	B	M	A	B	MB	MB	M	B	MB
	SSL/TLS	B	A	A	B	B	M	B	M	A	B	MB	B	M	B	MB
	BGP	B	A	A	B	B	M	B	M	A	B	MB	B	M	B	MB

Realizado por: Fiallos, Ricardo, 2022.

Tabla 30-4: Probabilidad de las amenazas de ataque de hombre en el medio - Sin plan de seguridad

	Amenazas	Dificultad	Motivación	Probabilidad
Ataques MiM	ARP Spoofing	B	M	A
	DNS Spoofing	M	M	M
	DHCP Spoofing	M	M	M
	SSL/TLS	M	A	A
	BGP	M	A	A

Realizado por: Fiallos, Ricardo, 2022.

Tabla 31-4: Riesgo de las amenazas de ataque de hombre en el medio - Sin plan de seguridad

	Amenazas	Impacto						Riesgo				
		[D]	[I]	[C]	[A]	[T]	[P]	[D]	[I]	[C]	[A]	[T]
Ataques MiM	ARP Spoofing	MB	MB	M	B	MB	A	B	B	A	M	B
	DNS Spoofing	MB	MB	M	B	MB	M	MB	MB	M	B	MB
	DHCP Spoofing	MB	MB	M	B	MB	M	MB	MB	M	B	MB
	SSL/TLS	MB	B	M	B	MB	A	B	M	A	M	B
	BGP	MB	B	M	B	MB	A	B	M	A	M	B

Realizado por: Fiallos, Ricardo, 2022.

4.3.3. Valoración de los riesgos con plan de seguridad aplicado

Tabla 32-4: Impacto de las amenazas de ataque de hombre en el medio - Con plan de seguridad

	Amenazas	**Degradación**					**Valor**					**Impacto**				
		[D]	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
Ataques MiM	ARP Spoofing	B	M	B	B	B	M	B	M	A	B	MB	MB	MB	B	MB
	DNS Spoofing	B	M	B	B	B	M	B	M	A	B	MB	MB	MB	B	MB
	DHCP Spoofing	B	M	B	B	B	M	B	M	A	B	MB	MB	MB	B	MB
	SSL/TLS	B	M	A	B	B	M	B	M	A	B	MB	MB	M	B	MB
	BGP	B	M	A	B	B	M	B	M	A	B	MB	MB	M	B	MB

Realizado por: Fiallos, Ricardo, 2022.

Tabla 33-4: Probabilidad de las amenazas de ataque de hombre en el medio - Con plan de seguridad

	Amenazas	Dificultad	Motivación	Probabilidad
Ataques MiM	ARP Spoofing	M	B	B
	DNS Spoofing	M	B	B
	DHCP Spoofing	M	B	B
	SSL/TLS	A	M	B
	BGP	A	M	B

Realizado por: Fiallos, Ricardo, 2022.

Tabla 34-4: Riesgo de las amenazas de ataque de hombre en el medio - Con plan de seguridad

	Amenazas	Impacto						Riesgo				
		[D]	[I]	[C]	[A]	[T]	[P]	[D]	[I]	[C]	[A]	[T]
Ataques MiM	ARP Spoofing	MB	MB	MB	B	MB	B	MB	MB	MB	B	MB
	DNS Spoofing	MB	MB	MB	B	MB	B	MB	MB	MB	B	MB
	DHCP Spoofing	MB	MB	MB	B	MB	B	MB	MB	MB	B	MB
	SSL/TLS	MB	MB	M	B	MB	B	MB	MB	M	B	MB
	BGP	MB	MB	M	B	MB	B	MB	MB	M	B	MB

Realizado por: Fiallos, Ricardo, 2022.

4.3.4. Riesgo potencial vs. Riesgo residual

Tabla 35-4: Riesgo de ataque sin plan de seguridad vs. Riesgo de ataque con plan de seguridad

Activos	Amenazas	Riesgo Potencial					Riesgo Residual				
		[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
con-inter-ser	ARP Spoofing	B	B	A	M	B	MB	MB	MB	B	MB
	DNS Spoofing	MB	MB	M	B	MB	MB	MB	MB	B	MB
	DHCP Spoofing	MB	MB	M	B	MB	MB	MB	MB	B	MB
	SSL/TLS	B	M	A	M	B	MB	MB	M	B	MB
	BGP	B	M	A	M	B	MB	MB	M	B	MB

Realizado por: Fiallos, Ricardo, 2022.

CAPÍTULO V

5. PROPUESTA

5.1. Plan de seguridad

Del método de análisis de riesgos obtuvimos las pautas necesarias para enmarcar el plan de seguridad encargado de materializar el tratamiento de riegos.

El plan de seguridad implanta o mejora la implantación de las salvaguardas más idóneas que lleven al impacto y al riesgo a niveles residuales. La implantación de las salvaguardas conlleva una serie de tareas, las mismas que se agrupan formando programas de seguridad. Cada programa de seguridad tiene su objetivo genérico en relación a las amenazas que trata y las salvaguardas que aborda (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012p).

5.1.1. Programas de Seguridad

Tomando en cuenta los riesgos a tratar y las salvaguardas localizadas, se ha estructurado el Plan de Seguridad en dos Programas de Seguridad que se detallan a continuación.

5.1.1.1. Programa de instalación y mantenimiento

Este programa recoge las salvaguardas que se aplican en las etapas de instalación, configuración y mantenimiento de las redes abiertas del estándar IEEE 802.11 b/g/n.

Objetivo: Reducir la probabilidad de ocurrencia de materialización de las amenazas que provengan de vulnerabilidades relacionadas a la instalación y mantenimiento de los equipos.

Salvaguardas: Este programa aborda el despliegue de las siguientes salvaguardas.
Aseguramiento de la disponibilidad: Para mejorar la disponibilidad del servicio se recomiendan las siguientes acciones:

- Capacitación al personal.
- Disponer de un UPS para los equipos implícitos en el servicio.
- Disponer de un enlace redundante de conectividad al internet.
- Instalar los equipos en lugares de acceso restringido a personal no autorizado.
- Instalación de un Firewall perimetral con capacidad de enrutamiento.

- Configuración del Punto de acceso inalámbrico en modo Bridge AP.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Cambio (Actualización y mantenimiento del software): Para el despliegue de esta salvaguarda se recomiendan las siguientes acciones:

- Capacitación al personal.
- La persona responsable de la red deberá mantener una suscripción activa a los canales oficiales de notificaciones de actualización y vulnerabilidades detectadas por el fabricante de los equipos instalados para la provisión del servicio.
- Se debe realizar revisiones periódicas de las actualizaciones disponibles para los equipos instalados.
- Previo a la instalación de una actualización se debe verificar si esta no traerá repercusiones negativas en la configuración o rendimiento actual del equipo.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Cambio (Actualización y mantenimiento del hardware): Para el despliegue de esta salvaguarda se recomiendan las siguientes acciones:

- Capacitación al personal.
- Revisión periódica del consumo de los recursos de los dispositivos que proveen el servicio.
- Revisión periódica del estado físico de los equipos.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Amenazas abordadas: El presente programa aborda las siguientes amenazas:

- E.21 Errores de mantenimiento Software.
- E.2 Errores del administrador.
- E.23 Errores de mantenimiento Hardware.
- E.24 Caída del sistema.
- E.25 Perdida de equipos.

Estimación de costes: Los costos detallados en la Tabla 4.14 se consideran de la implementación de una red inexistente, en el caso de redes existentes se deberá excluir los costos según corresponda.

Para los costos de salario del administrador, servicio de internet y servicio de internet redundante se consideró el costo anual.

Tabla 36-4: Estimación de costos Programa Implementación y Actualización

Ítem	Costo Unt.	Cantidad	Valor
Router inalámbrico	200	1	200
Firewall appliance	500	1	500
UPS	550	1	550
Cableado estructurado	0.8	100	80
Implementación de infraestructura	300	1	300
Servicio de internet	100	12	1200
Servicio redundante	100	12	1200
Salario del administrador	600	12	7200
Capacitación al personal	450	1	450
TOTAL (Dólares)			11680

Realizado por: Fiallos, Ricardo, 2022.

Subtareas a afrontar: Para que el programa tenga el efecto esperado se debe implementar adicionalmente un informe mensual de estado y mantenimiento de la red, el mismo que debe constar de lo siguiente:

- Inspección visual de los equipos.
- Revisión de las actualizaciones disponibles.
- Picos de saturación de los recursos.

Estimación del tiempo de ejecución: Se considera que el tiempo de implementación de la infraestructura es de 3 jornadas de trabajo.

El tiempo que tomará realizar las revisiones periódicas y el informe mensual se estiman de 5 horas al mes.

Estimación del Impacto y Riesgos residual: Tras la implantación del programa se espera reducir la probabilidad de las amenazas tratadas a parámetros bajos y muy bajos según el caso. Dado que el valor de los activos y la degradación de este valor tras la materialización de una amenaza no cambiaran por la aplicación de este programa el Impacto potencial se mantendrá para las amenazas tratadas. La matriz del riesgo potencial se muestra en la Tabla 15-4.

Tabla 37-4: Riesgo potencial de las amenazas sobre los activos

Activos	Amenazas	Impacto						Riesgo				
		[D]	[I]	[C]	[A]	[T]	[P]	[D]	[I]	[C]	[A]	[T]
Tratadas	E.21 Errores de mantenimiento HW	M	B				MB	B	MB			
	E.2 Errores del administrador	B	MB	MB			MB	MB	MB	MB		
	E.23 Errores de mantenimiento SW	M					MB	M				
	E.24 Caída del sistema	M					MB	B				
	E.25 Perdida de equipos	M					MB	B				

Realizado por: Fiallos, Ricardo, 2022.

Indicadores Los indicadores que nos permitirán valorar este programa son:

- Históricos de caídas del sistema.
- Informes mensuales.

5.1.1.2. Programa configuración de equipos

Este programa agrupa las herramientas recomendadas a ser usadas para disminuir la probabilidad de ocurrencia de materialización de las amenazas, cabe mencionar que a pesar de que las herramientas aquí sugeridas son de código abierto no se descarta el uso de herramientas privativas que cumplan con la funcionalidad requerida, el uso de estas u otras similares queda a consideración del lector.

Objetivo: Reducir la probabilidad de ocurrencia de materialización de las amenazas.
Salvaguardas: Este programa aborda el despliegue de las siguientes salvaguardas.

Herramienta de monitorización de tráfico: Esta salvaguarda incluye:

- Se realizarán monitorizaciones periódicas del tráfico en búsqueda de anomalías.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Protección de la integridad de los datos intercambiados: Esta salvaguarda incluye:

- Se denegará tráfico que no sea cifrado.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Protección de cifrado de la confidencialidad de los datos intercambiados: Esta salvaguarda incluye:

- Se denegará tráfico que no sea cifrado.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Internet: uso de? acceso a ?: Esta salvaguarda incluye:

- Se establecerá según el tipo de usuario final los contenidos aceptados y restringidos.
- Se establecerán mecanismos que restrinja el uso de la red para contenidos no aceptados.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).
Seguridad wireless (WiFi): Esta salvaguarda incluye:

- Se configurará un control de acceso al servicio por dirección física del dispositivo.
- Se establecerá y controlará el tiempo de uso máximo de uso de los recursos del servicio.
- Se configuran VLANs con número limitado de IP por VLAN.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Se aplican perfiles de seguridad: Para el despliegue de esta salvaguarda se recomiendan las siguientes acciones:

- Crear un usuario para el administrador del servicio.
- Establecer una contraseña robusta para el usuario del administrador.

Esta salvaguarda supone una eficacia de, Proceso Definido L3 (Tabla 13-4).

Amenazas abordadas: El presente programa aborda las siguientes amenazas:

- A.5 Suplantación de identidad.
- A.6 Abuso de privilegios de acceso.
- A.8 Difusión de software dañino.
- A.9 Re-encaminamiento de los mensajes.
- A.11 Acceso no autorizado.
- A.12 Análisis de tráfico.
- A.15 Modificación de la Información.
- A.22 Manipulación de programas.
- A.24 Denegación de servicios.

Estimación de costes: Para las configuraciones de los equipos se estima el esfuerzo en horas como el coste de implementación ya que en el programa Instalación y mantenimiento se determinó los costos de salarios y capacitación del administrador de la red, los costos detallados en la Tabla 16-4.

Tabla 38-4: Estimación de costos Programa Configuración

Ítem	Costo (horas)	Cantidad	Valor
Configuración IDS	16	1	16
Configuración IPS	16	1	16
Configuración del portal cautivo	16	1	16
Revisión de logs IDS	8	12	96
Revisión de logs IPS	8	12	96
Análisis de tráfico	12	12	144
Configuración de las reglas de firewall	16	1	16
Configuración del punto de acceso	4	1	16
Elaboración de informes	4	12	48
TOTAL			464

Realizado por: Fiallos, Ricardo, 2022.

Subtareas a afrontar: Para que el programa tenga el efecto esperado se debe implementar adicionalmente un informe mensual de revisión de logs, tráfico y configuraciones de la red, el mismo que debe constar de lo siguiente:

- Saturación de los recursos del servicio.
- Análisis de tráfico.
- Positivos del IDS.
- Positivos del IPS.
- Falsos positivos del IDS.
- Falsos positivos del IPS.

Estimación del Impacto y Riesgos residual: Tras la implantación del programa se espera reducir el impacto y riesgos potenciales a niveles residuales aceptables, como se muestras en las tabas siguientes.

Tabla 39-4: Impacto residual tras la aplicación del Programa configuración de equipos

Activos	Amenazas	Degradación					Valor					Impacto				
		[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
Tratadas	A.8 Difusión de software dañino	A	A	M			M	B	M	A	B	M	B	B		
	A.22 Manipulación de programas	A	A	M			M	B	M	A	B	M	B	B		
	A.6 Abuso de privilegio de acceso	A	A	M			M	B	M	A	B	M	B	B		
	A.11 Acceso no autorizado		M	M			M	B	M	A	B		MB	B		
	A.5 Suplantación de la identidad		A	A	A		M	B	M	A	B		B	M	A	
	A.9 Re-encaminamiento de los mensajes			A			M	B	M	A	B			M		
	A.12 Análisis de tráfico			M			M	B	M	A	B			B		
	A.15 Modificación de la información		A				M	B	M	A	B		B			
	A.24 Denegación de servicios	A					M	B	M	A	B	M				

Realizado por: Fiallos, Ricardo, 2022.

Tabla 40-4: Riesgo residual tras la aplicación del Programa configuración de equipos

	Amenazas	Degradación						Impacto				
		[D]	[I]	[C]	[A]	[T]	[P]	[D]	[I]	[C]	[A]	[T]
Tratadas	A.8 Difusión de software dañino	M	B	B			B	M	B	B		
	A.22 Manipulación de programas	M	B	B			B	M	B	B		
	A.6 Abuso de privilegio de acceso	M	B	B			MB	B	MB	MB		
	A.11 Acceso no autorizado		MB	B			MB		MB	MB		
	A.5 Suplantación de la identidad		B	M	A		MB		MB	B	M	
	A.9 Re-encaminamiento de los mensajes			M			B			M		
	A.12 Análisis de tráfico			B			A			M		
	A.15 Modificación de la información		B				MB		MB			
	A.24 Denegación de servicios	M					M	M				

Realizado por: Fiallos, Ricardo, 2022.

Indicadores Los indicadores que nos permitirán valorar este programa son:

- Logs del IDS.
- Logs del IPS.
- Análisis de tráfico.
- Históricos de ataques.
- Informes mensuales.

5.1.2. Plan de ejecución

El plan de ejecución requiere las siguientes actividades:

- Diseño e implementación de la infraestructura.
- Configuración de equipos.
- Revisión y mantenimiento.
- Capacitación del personal.

Para cada una de las actividades se presenta un cronograma de cometidos y una lista de control de tareas a cumplir.

5.1.2.1. Diseño e implementación de la infraestructura

El cronograma de cometidos propuesto se muestra en la Tabla 19-4.

Tabla 41-4: Cronograma Diseño e implementación de infraestructura

		Primera Semana				
Tareas	Diseño de infraestructura	X	X	X		
	Implementación de infraestructura			X	X	X

Realizado por: Fiallos, Ricardo, 2022.

La lista de control de tareas a cumplir se muestra en la Tabla 20-4.

Tabla 42-4: Lista de control Diseño e implementación de infraestructura

	La infraestructura cuenta con:	✓
Tareas	Restricción de acceso físico a personal no autorizado	
	UPS	
	Enlace redundante	
	Portal cautivo	
	VLANs	
	Cortafuegos	

Realizado por: Fiallos, Ricardo, 2022.

5.1.2.2. Configuración de equipos

El cronograma de cometidos propuesto se muestra en la Tabla 21-4.

Tabla 43-4: Cronograma Configuración de equipos

		Segunda Semana					**Tercera Semana**				
Tareas	Configuración del punto de acceso	X									
	Configuración de las reglas del cortafuegos		X	X	X						
	Configuración de VLANs				X	X	X				
	Configuración del portal cautivo							X	X	X	X

Realizado por: Fiallos, Ricardo, 2022.

La lista de control de tareas a cumplir se muestra en la Tabla 22-4.

Tabla 44-4: Lista de control Configuración de equipos

	Se configuraron en los equipos los siguientes parámetros:	✓
Punto de acceso	Perfil de administración	
	Contraseña robusta para el perfil de administración	
	Bloqueo para configurar por interface inalámbrica	
	Punto de acceso en modo AP bridge	
	Bloqueo de tráfico ARP en interface inalámbrica	
	Bloqueo para configurar por interface inalámbrica	
Cortafuegos	Perfil de administración	
	Contraseña robusta para el perfil de administración	
	Servidor DHCP	
	Parámetros de almacenamiento de logs	
	Reglas de restricción de tráfico inadecuado	
	Reglas de restricción de tráfico sin cifrado	

VLANs	Configurar VLANs	
	Determinar número máximo de usuarios simultáneos	
	Dividir los usuarios para cada VLAN	
Portal cautivo	Perfil de administración	
	Contraseña robusta para el perfil de administración	
	Control de acceso por dirección física	
	Control de acceso por usuario y contraseña	
	Control de acceso por tiempo limitado	
	Llave SSL para intercambio de contraseñas	
	Términos de uso del servicio	
	Tiempo máximo de uso del servicio	

Realizado por: Fiallos, Ricardo, 2022.

5.1.2.3. Revisión y mantenimiento

Las actividades de revisión y mantenimiento se deben realizar periódicamente el cronograma y lista de control de las tablas siguientes referencias a una actividad mensual.

Tabla 45-4: Cronograma Revisión y mantenimiento

		Primera Semana				
Tareas	Revisión de la infraestructura	X	X	X		
	Mantenimiento de infraestructura			X	X	X

Realizado por: Fiallos, Ricardo, 2022

La lista de control de tareas a cumplir se muestra en la Tabla 24-4.

Tabla 46-4: Lista de control Revisión y mantenimiento

	Se realizaron las siguientes actividades periódica:	✓
Revisión y Mantenimiento	Revisión de incidentes de seguridad reportados por el fabricante de los equipos	
	Picos de saturación del servicio en horas pico	
	Monitoreo de tráfico	
	Elaboro el informe mensual de revisión	
	Revisión física visual de los equipos	
	Limpieza de racks	

Realizado por: Fiallos, Ricardo, 2022.

5.1.2.4. Capacitación del personal

La capacitación del personal en tópicos referentes a la seguridad es importante para el mantenimiento de la infraestructura, para esto se sugiere el siguiente temario.

Tabla 47-4: Lista de control Capacitación del personal

	Se capacitó al personal en los siguientes aspectos:	✓
Tópicos	Manejo de reglas de cortafuegos	
	Revisión de logs del sistema	
	Configuración portal cautivo	
	Herramientas de pruebas de penetración	
	Herramientas de análisis de trafico	

Realizado por: Fiallos, Ricardo, 2022.

5.1.3. Riesgo potencial vs riesgo residual

En párrafos anteriores se determinaron tanto el riesgo potencial como el riesgo residual, ambos de acuerdo a la metodología Magerit que establece la reducción de los riesgos de acuerdo a la efectividad de las salvaguardas (Modernización Administrativa and e Impulso de la Administración Electrónica, 2012o).

Dado que, el presente trabajo determina una eficacia correspondiente a un proceso definido se espera una disminución de los riesgos en un factor de 60%. Como se muestra en la Tabla 26-4.

Tabla 48-4: Riesgo potencial vs. Riesgo residual

Activos	Amenazas	Riesgo Potencial					Riesgo Residual				
		[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
sw-net-wap	E.21 Errores de mantenimiento / actualización de programas (software)	A	M				B	MB			
	A.8 Difusión de software dañino	A	M	M			M	B	B		
	A.22 Manipulación de programas	A	M	M			M	B	B		
hw-net-wap	E.2 Errores del administrador	B	MB	MB			MB	MB	MB		
	E.23 Errores de mantenimiento / actualización de equipos (hardware)	A					M				
	E.24 Caída del sistema por agotamiento de recursos	M					B				
	E.25 Perdida de equipo	M					B				
	A.6 Abuso de privilegio de acceso	A	M	M			B	MB	MB		
	A.11 Acceso no autorizado		MB	B				MB	MB		
con-inter-ser	A.5 Suplantación de la identidad del usuario		M	A	MA			MB	B	M	
	A.9 Re-encaminamiento de los mensajes			A					M		
	A.12 Análisis de trafico			M					M		
	A.15 Modificación deliberada de la información		M					MB			
	A.24 Denegación de servicios	A					M				

Realizado por: Fiallos, Ricardo, 2022.

CONCLUSIONES

Los datos proporcionados por el INEC en la Encuesta Tecnológica TIC 2017, permite que el cálculo del riesgo inherente tenga la validez estadística necesaria para que los resultados del presente proyecto sean de utilidad en el tratamiento del riesgo de ataque Hombre en Medio en redes IEEE 802.11b/g/n de acceso libre.

El uso de las metodologías Magerit y OSSTMM V3 permiten enmarcar el desarrollo de la planificación de gestión del riesgo de ataque Hombre en Medio en redes IEEE 802.11b/g/n de acceso libre en estándares internacionales comprobados.

El riesgo potencial de ataque de Hombre en Medio en redes IEEE 802.11b/g/n de acceso libre previo a la aplicación del Plan de gestión de riesgo desarrollado en este proyecto de investigación es mayor que el riesgo residual posterior a la aplicación del Plan desarrollado.

El uso de un plan de seguridad informática basado en las metodologías Magerit y OSSTMM V3, disminuye el riesgo de ataque Hombre en el Medio en entornos de red IEEE 802.11b/g/n de acceso libre.

RECOMENDACIONES

Se recomienda que se evalué el valor del activo de información en torno a la información levantada en los futuros censos del INEC en la Encuesta Tecnológica TIC.

Se recomienda que en futuros trabajos de investigación se establezca un proceso de mejora continua en el plan de gestión de riesgos. Esto con la finalidad de mantener el plan actualizado a las estrategias de seguridad para abordar nuevas amenazas y vulnerabilidades.

Se recomienda el uso de la metodología Magerit para la elaboración de planes de gestión de riesgos informáticos tanto en entidades públicas como privadas.

Se recomienda llevar a cabo evaluaciones regulares de la seguridad utilizando metodologías como OSSTMM. Estas evaluaciones deben realizarse con la finalidad de garantizar que las medidas de seguridad sean efectivas y estén actualizadas.

GLOSARIO

Activo: Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (UNE 71504:2008).

Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (UNE 71504:2008).

Análisis de riesgos: Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización; también, proceso que permite comprender la naturaleza del riesgo y determinar el nivel de riesgo (UNE-ISO GUIA 73:2010 IN).

Ataque: Intento de destruir, exponer, alterar o inhabilitar un sistema de información o la información que el sistema maneja, o violar alguna política de seguridad de alguna otra manera (ISO/IEC 18043:2006).

Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados (UNE 71504:2008).

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados (UNE 71504:2008).

Impacto: Consecuencia que sobre un activo tiene la materialización de una amenaza (UNE-ISO GUIA 73:2010 IN).

Incidente de seguridad: Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información (UNE 71504:2008).

Integridad: Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada (UNE 71504:2008).

Salvaguarda: Procedimiento o mecanismo tecnológico que reduce el riesgo (UNE-ISO GUIA 73:2010 IN).

BIBLIOGRAFÍA

Asamblea Nacional. Código orgánico de la economía social de los conocimientos, creatividad e innovación. Nature, I:105, 2016.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, I:23, 2012a.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, I:24, 2012b.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro ii - método. Nature, II:25 – 49, 2012c.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, I:28, 2012d.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro iii - método. Nature, I:6, 2012e.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro iii - método. Nature, I:32 – 34, 2012f.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro iii - método. Nature, I:35, 2012g.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro iii - método. Nature, I:35, 2012h.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, I:7, 2012i.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, I:22, 2012j.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, III:36, 2012k.

Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro iii - guia de tecnicas. Nature, III:7, 2012l.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - metodo. Nature, I:29, 2012m.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - metodo. Nature, I:31, 2012n.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - catálogo de elementos. Nature, I:34, 2012o.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - catálogo de elementos. Nature, I:35, 2012p.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro ii - catálogo de elementos. Nature, II:7 – 13, 2012q.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro i - método. Nature, I:24, 2012r.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro ii - catálogo de elementos. Nature, II:19 – 22, 2012s.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro ii - catálogo de elementos. Nature, II:6, 2012t.
Dirección General de Modernización Administrativa and Procedimientos e Impulso de la Administración Electrónica. Magerit – versión 3.0. metodología de análisis y gestión de riesgos de los sistemas de información. libro iii - guia de tecnicas. Nature, III:6, 2012u.
ISECOM. Osstmm 3. Nature, I:20, 2010a.
ISECOM. Osstmm 3. Nature, I:33, 2010b.
ISECOM. Osstmm 3. Nature, I:45, 2010c.
ISECOM. Osstmm 3. Nature, I:56, 2010d.
ISECOM. Osstmm. Nature, I:33, 2010e.
ISECOM. Osstmm. Nature, I:33, 2010f.
ISO/IEC 18043:2006. Information technology.

Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. Papper, 1:1, 2014a.
Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. Papper, 1:2, 2014b.
Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. Papper, 1:3, 2014c.
Mauro Conti, Nicola Dragoni, and Viktor Lesyk. A survey of man in the middle attacks. Papper, 1:1–21, 2014d.
MINTEL. Libro blando de la sociedad y el conocimiento. Nature, I:5, 2018a.
MINTEL. Libro blando de la sociedad y el conocimiento. Nature, I:22, 2018b.
S. Plosz, A.Farshad, M. Tauber, C.Lesjak, T Ruprechter, and N. Pereira. Security vulnerabilities and risks in industrial usage of wireless communication. Papper, I:1, 2016a.
S. Plosz, A.Farshad, M. Tauber, C.Lesjak, T Ruprechter, and N. Pereira. Security vulnerabilities and risks in industrial usage of wireless communication. Papper, I:6, 2016b.
S. Plosz, A.Farshad, M. Tauber, C.Lesjak, T Ruprechter, and N. Pereira. Security vulnerabilities and risks in industrial usage of wireless communication. Papper, I:4, 2016c.
S. Plosz, A.Farshad, M. Tauber, C.Lesjak, T Ruprechter, and N. Pereira. Security vulnerabilities and risks in industrial usage of wireless communication. Papper, I:2 – 3, 2016d.
S. Plosz, A.Farshad, M. Tauber, C.Lesjak, T Ruprechter, and N. Pereira. Security vulnerabilities and risks in industrial usage of wireless communication. Papper, I:6, 2016e.
S. Plosz, A.Farshad, M. Tauber, C.Lesjak, T Ruprechter, and N. Pereira. Security vulnerabilities and risks in industrial usage of wireless communication. Papper, I:3, 2016f.
UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información.
UNE-ISO GUIA 73:2010 IN. Gestión del riesgo. Vocabulario.