Pontificia Universidad Católica del Ecuador

Facultad De Ingeniería

Escuela de Sistemas



TEMA:

Propuesta de aplicación de mecanismos de evaluación de riesgos mediante indicadores CVSS a un servidor de una Unidad de Gestión Tecnológica de una red VLAN.

AUTOR:

CARLOS DANIEL PÁEZ GALLEGOS

TRABAJO PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

QUITO, junio - 2023

DEDICATORIA

Querida mamá, querido papá, y a toda mi amada familia,

Hoy, en este importante momento de mi vida, quiero expresar mi más profunda gratitud y amor hacia ustedes. Sin su apoyo incondicional y su constante aliento, no estaría aquí, celebrando la culminación de mi tesis.

Desde mi más tierna infancia, ustedes han sido mi inspiración y mis pilares. Su amor, dedicación y sacrificio han sido los cimientos sobre los cuales he construido mi camino académico. Cada logro que he alcanzado es gracias a su constante respaldo y creencia en mí. Siempre han estado ahí para celebrar mis triunfos y para sostenerme en momentos de desafío.

Mamá y papá, su fe en mis habilidades y su valioso consejo me han dado la confianza necesaria para perseguir mis sueños. Han sido mis guías en la búsqueda del conocimiento y me han enseñado la importancia del esfuerzo y la perseverancia. Su amor incondicional me ha dado fuerza para superar los obstáculos y para mantenerme enfocado/a en este arduo camino de la investigación.

AGRADECIMIENTO

Hoy quiero expresar mi más sincero agradecimiento a cada uno de ustedes por haber sido parte de este importante momento en mi vida. No puedo expresar con palabras la gratitud que siento hacia cada uno de ustedes por su tiempo, dedicación y conocimientos que han brindado durante este proceso.

Agradezco profundamente a mi director de tesis, por su guía, paciencia y apoyo incondicional a lo largo de este camino. Su sabiduría, experiencia y pasión por la investigación han sido una inspiración para mí. Gracias por creer en mí y por brindarme las herramientas necesarias para llevar a cabo este proyecto de manera exitosa.

También quiero agradecer a los miembros del jurado, por su disposición para evaluar mi trabajo y brindarme valiosos comentarios y sugerencias. Su experiencia y conocimientos han sido fundamentales para enriquecer mi investigación y para ayudarme a alcanzar un mayor nivel de excelencia académica.

RESUMEN

En el trabajo realizado, se ha llevado a cabo un análisis de riesgos utilizando la metodología MAGERIT para evaluar la seguridad de los activos de una organización. Se han identificado los activos relevantes, como switches, routers, estaciones de trabajo, servidor de gestión de usuarios y servidor de correos, se ha evaluado su impacto potencial y residual.

Se han identificado vulnerabilidades que podrían verse afectadas por amenazas en los activos de la Unidad de Gestión Tecnológica tales como ataques de denegación de servicio, acceso no autorizado, robo de información y fallos en la disponibilidad de los servicios. A partir de esto, se han propuesto salvaguardas para mitigar los riesgos identificados, como la implementación de autenticación segura, políticas de contraseñas fuertes, desactivación de servicios no seguros, configuración segura de servidores y actualizaciones regulares del sistema operativo.

Se han realizado estimaciones del impacto potencial y residual, considerando la magnitud del impacto y la probabilidad de ocurrencia de las amenazas. Además, se ha aplicado el marco de puntuación CVSS para evaluar la gravedad de las vulnerabilidades identificadas y se han presentado los resultados como evidencia del riesgo que enfrentan las empresas al no mantener una adecuada ciberseguridad.

ÍNDICE

CAPÍTULO I: INTRODUCCIÓN 1

1. MARCO DE REFERENCIA 1

1.1. JUSTIFICACIÓN 1

1.2. Planteamiento del problema 1

1.3. Objetivo General 1

1.4. Objetivos Específicos 2

1.5. Alcance 2

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA 3

2. MARCO TEÓRICO 3

2.1. Análisis de riesgos 3

2.1.1. Beneficios de realizar un análisis de vulnerabilidades 3

2.2. Importancia de la seguridad informática 4

2.2.1. Seguridad de red 4

2.2.2. Seguridad de aplicaciones 5

2.3. VLAN 6

2.4. Modelo OSI 8

2.5. Kali Linux 10

2.6. Common Vulnerability Scoring System 3.0 10

2.7. Grupo de métricas de CVSS 3.0 11

2.7.1. Métrica base 11

2.7.2. Métrica temporal....14
2.7.3. Métrica de entorno....16
2.8. Funcionamiento de las métricas de evaluación....17
CAPÍTULO III: DESARROLLO....19
3. METODOLOGÍA....19
3.1. Enfoque de la Investigación....19
3.1.1. Enfoque Cualitativo....19
3.2. Diseño de Investigación....20
3.2.1. Diseño no experimental....20
3.3. Nivel de la investigación....21
3.3.1. Investigación Exploratoria....21
3.4. Tipo de investigación....21
3.4.1. Investigación bibliográfica....21
3.5. Modalidad de la investigación....22
3.5.1. Modalidad de la propuesta tecnológica....22
3.6. Descripción de la propuesta....22
3.7. Población y muestra....23
3.8. Muestreo no probabilístico....23
3.9. Técnica e instrumentos....24
3.10. Método de análisis de riesgos (MAGERIT)....24
3.11. Limitaciones de la investigación....27

CAPÍTULO IV: IMPLEMENTACIÓN 29
4. Formalización de las actividades 29
4.1. Tarea MAR 1: Caracterización de los activos.....29
4.2. Tarea MAR 2: Caracterización de las amenazas 31
4.2.1. Escaneo de vulnerabilidades con Nessus 31
4.2.2. Categorización de amenazas 32
4.2.3. Mapa de riesgos.....34
4.3. Tarea MAR 3: Caracterización de las salvaguardas.....34
4.3.1. Identificación Salvaguardas.....35
4.4. Tarea MAR 4: Estimación del estado de riesgo 35
4.4.1. Estimación del Impacto 36
4.4.2. Estimación del riesgo 36
4.5. Resultados.....36
CONCLUSIONES Y RECOMENDACIONES.....38
Conclusiones.....38
Recomendaciones.....39
BIBLIOGRAFÍA 40
ANEXOS 42
Anexo A: Adjuntar anexos si los necesita para la elaboración de la tesis 42
1.1. Desarrollo de la entrevista 42

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE FIGURAS

Figura 1. 14

Grupo de métricas base 14

Figura 2. 16

Grupo de métricas temporales 16

Figura 3. 17

Grupo de métricas de ambiente....17

Figura 4. 18

Diagrama de cómo se obtiene el puntaje en CVSS 18

ÍNDICE DE TABLAS

Tabla 1. 30

Caracterización de los activos 30

Tabla 2. 32

Vulnerabilidades encontradas mediante escaneo básico de red....32

Tabla 3. 32

Posibles amenazas a las que se enfrente el sistema....32

Tabla 4. 34

Desarrollo del mapa de riesgos para el sistema 34

Tabla 5. 35

Salvaguardas propuestas para los activos 35

Tabla 6. 36

Impacto estimado en los activos....36

Tabla 7. 36

Riesgo estimado en los activos 36

CAPÍTULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA

1.1. JUSTIFICACIÓN

En la actualidad existen muchas vulnerabilidades en las configuraciones de los dispositivos que forman parte de las redes empresariales y sistemas de información que podrían ser aprovechados por ciberdelincuentes, lo que podría poner en riesgo la información confidencial de los ciudadanos y empresas, con base en lo planteado, el Esquema Gubernamental de Seguridad de la Información y la Estrategia Nacional de Ciberseguridad del Ecuador busca aplicar en todas las empresas las buenas prácticas para el manejo de la información de todos los ciudadanos, con ello se plantean métodos con los cuales debe regirse cualquier lugar que maneje información en especial aquellos sectores que tengan grandes de volúmenes de datos ya que esta es de carácter sensible.

1.2. Planteamiento del problema

La red de la Unidad de Gestión Tecnológica de una organización es vulnerable a diversos riesgos de seguridad, lo que puede comprometer la privacidad y seguridad de los datos sensibles que maneja. La falta de mecanismos efectivos de evaluación de riesgos hace que la Unidad de Gestión Tecnológica no pueda identificar y mitigar eficazmente estos riesgos. Por ello surge la siguiente problemática: ¿Cómo se puede aplicar el mecanismo de evaluación de riesgos mediante CVSS en la red VLAN de una Unidad de Gestión Tecnológica para identificar y mitigar los riesgos de seguridad de los datos sensibles?

1.3. Objetivo General

- Analizar los riesgos encontrados en el servidor de la unidad de gestión tecnológica aplicando mecanismos de evaluación de riesgos y CVSS para el análisis de

vulnerabilidades, y con ello evaluar la seguridad de la información incrementado la confianza de los usuarios en la organización.

1.4. Objetivos Específicos

- Realizar un análisis de la situación actual mediante un escaneo de vulnerabilidades para obtener información de un servidor de la red.

- Aplicar el marco de puntuación CVSS a los resultados obtenidos del análisis de vulnerabilidades para determinar mediante la metodología MAGERIT el nivel de riesgo de los activos de la empresa.

- Desarrollar las MAR para categorizar los activos, las amenazas y exponer los resultados como evidencia del riesgo que corren las empresas al no tener salvaguardas ni una estimación del riesgo de la red.

1.5. Alcance

El presente trabajo se limita a la aplicación de mecanismos de evaluación de riesgos en el departamento encargado de la infraestructura tecnológica de una empresa, el tiempo de desarrollo debe ser entre 1 a 3 meses y se enfoca en aquellos activos que sean estrictamente parte de la Unidad de Gestión Tecnológica y que presenten una cantidad considerable de vulnerabilidades para evitar la indisponibilidad del servicio y mantener el flujo de trabajo constante.

CAPÍTULO II: FUNDAMENTACIÓN TEÓRICA

2. MARCO TEÓRICO

2.1. Análisis de riesgos

Para Ambi BST (2020) el análisis de riesgos informáticos se refiere a la evaluación de las diferentes amenazas que pueden afectar a nivel informático y provocar situaciones de riesgo para el negocio, como robos de datos, intrusiones o ataques externos que puedan interrumpir el funcionamiento de los sistemas y generar periodos de inactividad en la empresa. El análisis de riesgos ayuda a prevenir este tipo de situaciones negativas y contempla una serie de factores esenciales para lograr este objetivo, dentro de estos factores existe el análisis de vulnerabilidades, presentes tanto en un sistema de la información, como en los equipos físicos donde está instalado este sistema.

2.1.1. Beneficios de realizar un análisis de vulnerabilidades

En la actualidad, la seguridad informática abarca tanto la implementación de productos que impidan que las amenazas, cada vez más complejas, comprometan la red, como la labor de ingenieros capacitados para detectarlas y procesos de respuesta en caso de detectar posibles amenazas IDRIC (2022). El análisis de vulnerabilidades es un procedimiento esencial para determinar, clasificar y priorizar las debilidades en la infraestructura de TI de una organización, a continuación, se presentan los beneficios de realizarlo:

- Identifica las vulnerabilidades antes que los ciberdelincuentes
- Ayuda a definir el nivel de riesgo al que se expone tu infraestructura
- Gestiona y asigna recursos de forma eficiente
- Ahorra tiempo y dinero
- Mejora los sistemas de seguridad

- Ayuda a cumplir con los requisitos de protección de datos
- Aumenta la credibilidad ante clientes y socios

2.2. Importancia de la seguridad informática

El tema de seguridad informática no es nuevo sin embargo es un tema que no pierde interés en el transcurso del tiempo Gamboa Suarez (2020) señaló que la seguridad informática tiene como objetivo proteger la información personal, empresarial y gubernamental, no solo en la red, sino también en dispositivos de uso diario como teléfonos móviles, tabletas, computadoras de escritorio y portátiles, de posibles amenazas que puedan poner en riesgo los datos almacenados o transportados. En este sentido, la ciberseguridad no solo debe enfocarse en la prevención de ataques, sino también en su detección y corrección, con el fin de minimizar los riesgos de exposición de la información y garantizar la confianza de los usuarios.

Existen diversas categorías de la seguridad de la información, dado que el mundo tecnológico se convirtió en un campo tan amplio y ya no basta con desarrollar soluciones de manera general, a continuación se presentan las diversas ramas de seguridad de la informática:

2.2.1. Seguridad de red

Según Gamboa Suarez (2020), las medidas de seguridad informática y ciberseguridad tienen como propósito proteger una red informática de posibles intrusos, ya sean atacantes dirigidos o un programa maligno oportunista. Esto implica autorizar el acceso a los datos almacenados en la red, los cuales son controlados por un administrador. En este sentido, los usuarios pueden elegir o recibir una identificación y contraseña para autenticarse y acceder a la información y programas dentro de sus permisos.

2.2.2. Seguridad de aplicaciones

Gamboa Suarez (2020) señala que la seguridad de las aplicaciones se refiere al proceso de mejorar y garantizar su seguridad mediante la identificación y corrección de vulnerabilidades. Aunque gran parte de este proceso se lleva a cabo durante la fase de desarrollo, también incluye herramientas y métodos para proteger las aplicaciones después de su implementación. El enfoque de la seguridad de las aplicaciones es mantener los dispositivos y el software libres de amenazas, ya que una aplicación afectada o mal diseñada puede permitir el acceso a datos que se supone debe proteger. En este sentido, la seguridad efectiva debe comenzar en la etapa de diseño, mucho antes de la implementación de un programa o dispositivo.

2.2.3. Seguridad de la información

La protección de la información mediante medidas preventivas y reactivas se conoce como seguridad de la información, la cual busca mantener la confidencialidad, integridad y autenticidad de los datos, ya sea durante su almacenamiento o tránsito. Es importante destacar que la seguridad de la información abarca un espectro más amplio en comparación con la seguridad informativa, la cual se enfoca específicamente en la Ciberseguridad y no involucra otros aspectos de importancia global. (Gamboa Suarez, 2020).

2.2.4. Seguridad Operativa

La Seguridad Operativa se refiere a un conjunto de procedimientos que se emplean para minimizar los riesgos asociados con la información, el software y los equipos, incluyendo procesos y decisiones que se utilizan para gestionar los recursos de datos. Esto incluye la autorización de acceso a una red para los usuarios, así como los procedimientos para determinar cómo y dónde se puede almacenar y compartir la información. La capacitación y

concienciación de los empleados sobre los riesgos y la prevención son fundamentales en la Seguridad Operativa. (Gamboa Suarez, 2020).

2.2.5. Recuperación ante desastres y la continuidad del Negocio

La capacidad de una organización para responder a un incidente de seguridad informática o cualquier otro evento que interrumpa sus operaciones y cause la pérdida de datos o información se conoce como respuesta a incidentes. Las políticas de recuperación ante desastres establecen cómo la organización restaurará sus operaciones y datos para recuperar su capacidad operativa anterior al evento. La continuidad del negocio es el plan que utiliza la organización para seguir operando sin ciertos recursos. (Gamboa Suarez, 2020).

2.2.6. Capacidad del Usuario

El aspecto de la seguridad informática que involucra a las personas es el enfoque de este tema. Las prácticas de seguridad descuidadas pueden provocar la introducción de virus o un programa maligno en sistemas seguros. Por lo tanto, es importante instruir a los usuarios en buenas prácticas de seguridad, como evitar abrir archivos adjuntos de correos electrónicos sospechosos y no conectar dispositivos USB desconocidos, entre otras enseñanzas vitales para la seguridad de cualquier organización. La educación de los usuarios es esencial para la prevención de incidentes de seguridad. (Gamboa Suarez, 2020).

2.3. VLAN

De acuerdo con De Luz (2023), una VLAN es una "red lógica independiente" creada dentro de una red física. La segmentación de la red mediante el uso de VLAN permite una administración más eficiente de los recursos de red y una mayor seguridad consiguiendo así que la red sea más flexible y escalable.

Para una mejor eficiencia las redes físicas deben segmentarse acorde el número de departamentos que vayan a funcionar en las empresas, a continuación, se detallan una serie de características intrínsecas de una VLAN

2.3.1. **Seguridad:** Según De Luz (2023), las VLAN tienen la capacidad de crear redes lógicamente independientes y pueden ser aisladas para restringir el acceso a Internet y negar el tráfico de una VLAN a otra, por defecto no se permite que las VLAN intercambien tráfico con otras Vlan, y se requiere un router o un switch multicapa en el nivel de red (L3) para habilitar el enrutamiento entre Vlan, permitiendo así la comunicación entre ellas cuando sea necesario.

2.3.2. **Segmentación:** Para De Luz (2023), las VLAN permiten la segmentación de todos los equipos en diferentes subredes, asignando a cada subred una VLAN diferente, por ejemplo, es posible crear una subred de gestión interna para routers, switches y puntos de acceso, una subred para administradores, otra para dispositivos IoT y una más para invitados. De esta manera, se puede segmentar la red principal en subredes para que cada una pueda utilizar las comunicaciones según sus necesidades.

2.3.3. **Flexibilidad:** Según De Luz (2023), se puede redistribuir los equipos entre subredes de manera simple, y gestionar las políticas de comunicación entre VLANS para denegar tráfico.

2.3.4. **Optimización de la red:** Según De Luz (2023), la segmentación de redes en subredes más pequeñas mediante el uso de VLAN puede mejorar el rendimiento de la red al reducir la cantidad de mensajes de broadcast transmitidos a todos los equipos, lo que puede hacer que la red se congestione y reducir su rendimiento. Las VLAN también pueden reducir la necesidad de enviar tráfico a destinos innecesarios, lo que puede reducir el volumen de tráfico y mejorar el rendimiento de la red. Además, las VLAN pueden reducir la cantidad de routers necesarios en la red al crear dominios de

transmisión utilizando switches en lugar de routers, lo que puede mejorar el rendimiento al reducir la latencia.

2.3.5. **Reducción de costes:** En concordancia con De Luz (2023), es factible disminuir los costos de actualización de las redes al emplear de manera efectiva los enlaces y el ancho de banda disponible, lo que conduce a reducir la necesidad de actualizaciones costosas. Una alternativa es la implementación de VLAN, las cuales permiten establecer dominios de transmisión para evitar el uso de routers costosos, lo que contribuye a una disminución adicional de los costos.

2.3.6. **Mejor eficiencia del personal de TI:** Según lo expuesto por De Luz (2023), una ventaja de la implementación de VLAN es que pueden mejorar la gestión de la red al permitir que distintos usuarios compartan una misma VLAN. Además, al agregar un nuevo switch, este adoptará automáticamente las políticas y procedimientos preestablecidos de la VLAN correspondiente, lo que facilitará su manejo. Por otro lado, asignar nombres a cada VLAN ayuda a identificar de manera más clara su función específica.

2.3.7. **Administración de aplicaciones y proyectos simples:** De Luz (2023) explica que, las VLAN facilitan la administración de aplicaciones y proyectos, reducen costos de actualización de red y simplifican tareas de reconfiguración. Sin embargo, su implementación requiere herramientas de administración eficientes y añade una capa de complejidad administrativa al tener que gestionar grupos de trabajo virtuales.

2.4. Modelo OSI

Acorde a Profesional Review (2018) OSI es un modelo orientado a desentrañar el funcionamiento de la infraestructura de comunicaciones de cualquier Red, este modelo explica de manera profunda como se logra dar la comunicación entre los distintos tipos de dispositivos que pertenecen a una red, comúnmente la infraestructura de red consta de los siguientes

dispositivos: Switch, Acces Point, Routers, Estaciones de trabajo, Firewalls, Sistemas de detección y prevención de intrusiones, Gateways, Modems, Hubs, etc.

Según Profesional Review (2018) el modelo OSI se compone de varias capas por las cuales los datos fluyen entre los distintos dispositivos de la red, una vez finalizado su recorrido llegan a la capa de aplicación donde los datos son fácilmente reconocibles por el usuario final.

2.4.1. Niveles OSI orientados a red

Capa física: Para Profesional Review (2018). Esta capa se encarga de la transmisión física de los datos a través del medio de comunicación. Se encarga de la conexión y desconexión física entre los dispositivos.

Capa de enlace de datos: Acorde a Profesional Review (2018) esta capa se encarga de la transmisión de datos entre dos dispositivos en la misma red. Se encarga de dividir los datos en tramas y de realizar la corrección de errores.

Capa de red: Acorde a Profesional Review (2018) Esta capa se encarga de la transmisión de datos entre dos dispositivos que se encuentran en redes diferentes. Se encarga del enrutamiento de los paquetes, es decir, de determinar la mejor ruta para que los datos lleguen a su destino.

Capa de transporte: Acorde a Profesional Review (2018) esta capa se encarga de la entrega de los datos a su destino final. Se encarga de asegurar la entrega de los datos y de controlar el flujo de información.

2.4.2. Niveles OSI orientados a aplicación

Capa de sesión: Acorde a Profesional Review (2018) esta capa se encarga de establecer, mantener y finalizar las sesiones entre dos dispositivos. Se encarga de mantener la comunicación entre los dispositivos durante todo el proceso.

Capa de presentación: Acorde a Profesional Review (2018) esta capa se encarga de la presentación de los datos en un formato que pueda ser entendido por los dispositivos receptores. Se encarga de la codificación y decodificación de los datos.

Capa de aplicación: Acorde a Profesional Review (2018) esta capa se encarga de la comunicación entre las aplicaciones y el usuario final. Se encarga de la gestión de las diferentes aplicaciones y servicios que se ejecutan en la red.

2.5. Kali Linux

Según Altube (2021) Kali Linux es una distribución de Linux especializada en cuestiones de seguridad. Se basa en Debian y ofrece una amplia gama de herramientas para llevar a cabo pruebas y análisis de seguridad, incluyendo análisis de redes, ataques inalámbricos, y análisis forenses, entre otros. Esta distribución fue desarrollada por Mati Aharoni y Devon Kearns de Offensive Security, quienes reescribieron BackTrack, otra distribución de Linux utilizada para estos fines. Kali Linux es muy popular y es ampliamente utilizada tanto a nivel personal como profesional, ya que ofrece herramientas como Foremost, Wireshark, Maltigo as-Aircrack-ng, Kismet, entre otras, para satisfacer las necesidades de los usuarios.

2.6. Common Vulnerability Scoring System 3.0

A medida que avanza la tecnología, surgen retos de seguridad que deben ser superados. Con el auge de las telecomunicaciones, la seguridad de la información no solo está disponible para ser vulnerada de manera local, sino también global. Con ello, surge un grupo de métricas para evaluar el riesgo de una red conocidas como Common Vulnerability Scoring System (CVSS). Acorde a Welivesecurity (2014) CVSS es un marco de referencia que permite medir de manera cuantitativa el nivel de riesgo asociado a una vulnerabilidad informática en términos de confidencialidad, integridad y disponibilidad.

Este marco considera diferentes factores de impacto y explotación, los cuales son valorados mediante una serie de métricas que permiten determinar un puntaje numérico que representa el nivel de riesgo de la vulnerabilidad. Esto permite a los profesionales de la seguridad informática priorizar y gestionar de manera más efectiva los riesgos de seguridad en sus redes y sistemas.

2.7. Grupo de métricas de CVSS 3.0

2.7.1. Métrica base

Las métricas base son aquel tipo de métricas que no varían en el tiempo, esto quiere decir que son características intrínsecas de los objetos vulnerables, tales como hardware y software.

Exploitability metrics

En palabras de FIRST (2019) las métricas de Explotación reflejan las características de lo que es vulnerable, a lo que nos referimos formalmente como el componente vulnerable. Por lo tanto, cada una de las métricas de Explotabilidad enumeradas a continuación debe puntuarse en relación con el componente vulnerable y reflejar las propiedades de la vulnerabilidad que conducen a un ataque exitoso.

Attack Vector

Según FIRST (2019) refleja el ambiente en el que es posible el aprovechamiento de vulnerabilidades. Este valor de métrica (y, en consecuencia, la puntuación base) incrementa cuanto más lejano (lógica y físicamente) pueda estar un posible atacante para utilizar el componente vulnerable, con esa premisa se supone que la cantidad de atacantes potenciales para una vulnerabilidad que podría explotarse a través de una red es mayor que la cantidad de atacantes potenciales que podrían explotar una vulnerabilidad que requiere acceso físico a un dispositivo.

Attack Complexity

Acorde a FIRST (2019) son las condiciones fuera del control del atacante que deben existir para aprovechar la vulnerabilidad, como se describe a continuación, tales condiciones pueden requerir la recopilación de más información sobre el objetivo o excepciones computacionales. Si se requiere una configuración específica para que un ataque tenga éxito, las métricas base deben puntuarse asumiendo que el componente vulnerable está en esa configuración.

Privileges Required

Para FIRST (2019) es el nivel de privilegios que debe poseer un atacante antes de aprovechar con éxito la vulnerabilidad, la puntuación base es mayor si no se requieren privilegios.

User Interaction

Según FIRST (2019) se refiere a la necesidad de que un usuario humano, que no sea el mismo atacante, participe para comprometer exitosamente el componente vulnerable, la importancia de esto se basa en si la vulnerabilidad se puede aprovechar únicamente a voluntad del perpetrador o si un usuario independiente debe participar de alguna manera.

Scope

Para FIRST (2019) la métrica de alcance captura si una vulnerabilidad en un componente vulnerable afecta los recursos en componentes más allá de su alcance de seguridad.

Impact metric

En palabras de FIRST (2019) las métricas de impacto capturan los efectos de una vulnerabilidad aprovechada con éxito en el elemento que padece la peor consecuencia y que

está asociado de manera más directa y predecible con el ataque. Los analistas deben acotar los impactos a un resultado final prudente que estén seguros de que un atacante puede lograr.

Confidentiality Impact

Para FIRST (2019) consiste en el impacto en la confidencialidad de los medios de información administrados por un elemento de software debido a una vulnerabilidad aprovechada con éxito. Se refiere a restringir el acceso y la difusión de la información solo a usuarios autorizados, y evitarlo en usuarios no autorizados.

Integrity Impact

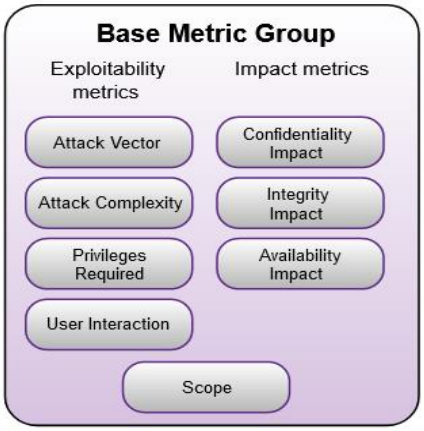
Según FIRST (2019) consiste en medir el impacto respecto a la integridad de una vulnerabilidad aprovechada con éxito, la integridad se refiere a la confiabilidad y veracidad de la información.

Availability Impact

Según FIRST (2019) radica en medir el impacto en la disponibilidad del elemento afectado como resultado de una vulnerabilidad aprovechada con éxito. Si bien las métricas de impacto de confidencialidad e integridad se aplican a la pérdida de confidencialidad o integridad de los datos (por ejemplo, información, archivos) utilizados por el componente afectado, esta métrica se refiere a la pérdida de disponibilidad del propio componente afectado, como un servicio en red (web, base de datos, correo electrónico). FIRTS (2019) explica que la disponibilidad se refiere a la accesibilidad de los recursos de información, los ataques que consumen el ancho de banda de la red, los ciclos del procesador o el espacio en disco afectan la disponibilidad de un componente afectado.

Figura 1.

Grupo de métricas base



Nota: tomado de FIRST, (https://www.first.org/cvss/v3.1/specification-document).

2.7.2. Métrica temporal

Para FIRST (2019) Las métricas temporales refleja las características de una vulnerabilidad que puede cambiar con el tiempo, pero no entre los entornos de los usuarios.

Exploit Code Maturity

Según FIRST (2019) acá lo importante es la probabilidad de que se aproveche la vulnerabilidad presente y, por lo general, se basa en el estado actual de las técnicas de explotación, la disponibilidad del código de explotación o la explotación activa. Por ello FIRST (2019) determina que la disponibilidad pública de un código de explotación fácil de usar aumenta la cantidad de atacantes potenciales al incluir a aquellos que no están calificados, lo que aumenta la gravedad de la vulnerabilidad.

Es entonces que FIRTS (2019) explica que el código de explotación disponible puede pasar de una demostración de prueba de concepto a un código de explotación que tiene éxito en la explotación de la vulnerabilidad de manera consistente.

Remediation Level

En palabras de FIRST (2019) el nivel de compensación de una vulnerabilidad es un factor importante a priorizar. La vulnerabilidad típica no se corrige cuando se publica inicialmente. Las soluciones provisionales o las revisiones pueden ofrecer soluciones provisionales hasta que se emita un parche o una actualización oficial. Cada una de estas etapas respectivas ajusta el puntaje temporal hacia abajo, lo que refleja la urgencia decreciente a medida que la remediación se vuelve definitiva.

Report Confidence

Según FIRST (2019) aquí se evalúa el grado de credibilidad en la existencia de la vulnerabilidad y la confianza de los detalles técnicos conocidos, a veces solo se da a conocer la existencia de vulnerabilidades, pero sin información específica.

Entonces FIRTS (2019) indica que la vulnerabilidad puede ser corroborada posteriormente por una investigación que sugiera dónde puede estar la vulnerabilidad, aunque la investigación puede no ser segura. Finalmente, una vulnerabilidad puede confirmarse mediante el reconocimiento por parte del autor o proveedor de la tecnología afectada.

Figura 2.

Grupo de métricas temporales



Nota: tomado de FIRST, (https://www.first.org/cvss/v3.1/specification-document).

2.7.3. Métrica de entorno

Según FIRST (2019) los analistas pueden personalizar el puntaje CVSS según la importancia del activo afectado para la organización, esto se mide en términos de controles de seguridad complementarios/alternativos implementados, confidencialidad, integridad y disponibilidad. FIRTS (2019) explica que para lograr esto, se utilizan métricas equivalentes modificadas de las métricas base. Los valores de estas métricas modificadas se asignan según la ubicación del componente dentro de la infraestructura de la organización.

Security Requirement

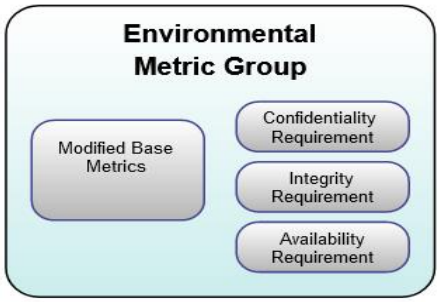
Estas métricas en palabras de FIRST (2019) se miden en términos de confidencialidad, integridad y disponibilidad. Es decir, si un activo de TI respalda una función comercial para la cual la Disponibilidad es más importante, el analista puede asignar un mayor valor a la Disponibilidad en relación con la Confidencialidad y la Integridad. Cada requisito de seguridad tiene tres valores posibles: bajo, medio o alto.

Modified Base Metrics

Conforme avanza el proceso FIRST (2019) explica que el analista puede anular las métricas base individuales en función de las características específicas del entorno de un usuario. Las características que afectan la Explotación, el Alcance o el Impacto se pueden reflejar a través de una Puntuación Ambiental modificada apropiadamente.

Figura 3.

Grupo de métricas de ambiente



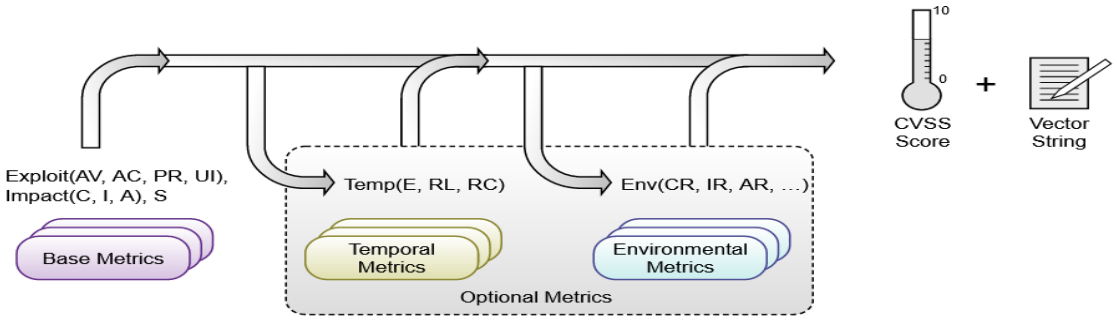
Nota: tomado de FIRST, (https://www.first.org/cvss/v3.1/specification-document).

2.8. Funcionamiento de las métricas de evaluación

Depende de un analista asignar valores a las métricas base, lo cual da paso al proceso para determinar el índice de riesgo del activo que está siendo evaluado según la vulnerabilidad detectada, Según FIRST (2019) El puntaje Base luego puede ser refinado al puntuar las métricas temporales y ambientales para reflejar de manera más precisa el riesgo que representa una vulnerabilidad para el entorno de un usuario. Sin embargo, puntuar las métricas Temporales y Ambientales no es obligatorio.

Figura 4.

Diagrama de cómo se obtiene el puntaje en CVSS



Nota: tomado de FIRST, (https://www.first.org/cvss/v3.1/specification-document).

CAPÍTULO III: DESARROLLO

3. METODOLOGÍA

Acorde a Hernández (2020) La metodología se refiere al conjunto de métodos y técnicas utilizados en una investigación o estudio. Es el proceso empleado para recolectar, analizar y obtener resultados que respondan a la pregunta de investigación. La metodología debe ser rigurosa, sistemática y permitir la replicación de los resultados por otros investigadores. Seguir una metodología adecuada es crucial para asegurar la validez y confiabilidad de los hallazgos.

3.1. Enfoque de la Investigación

Acorde a Hernández (2020) Basándonos en las características y necesidades identificadas en la investigación, se actualizará la metodología adoptando un enfoque cualitativo. El objetivo de este enfoque es proporcionar información relevante a la comunidad educativa de la Carrera de Pedagogía de las Ciencias Experimentales Informática acerca de los proyectos y actividades académicas y administrativas. Esta actualización se llevará a cabo utilizando un enfoque cualitativo

3.1.1. Enfoque Cualitativo

Acorde a Hernández (2020) El enfoque utilizado en esta investigación fue cualitativo, ya que no se realizará ningún análisis estadístico. Este enfoque nos permitió examinar la viabilidad de desarrollar un sitio web informativo que permita revisar las actividades de la Carrera de Pedagogía de las Ciencias Experimentales Informática, a través del estudio de acciones, opiniones y criterios de la comunidad educativa.

En base a lo anterior, Hernández (2020) indica que llevamos a cabo una investigación para identificar las necesidades de la Carrera de Pedagogía de las Ciencias Experimentales Informática, particularmente la falta de información actualizada sobre las actividades

académicas y extracurriculares de la carrera. Por lo tanto, resulta crucial contar con un sitio web informativo que mejore la comunicación entre estudiantes, docentes y personal administrativo de la institución.

Para Hernández (2020) Cada enfoque de investigación implica compromisos ontológicos, epistemológicos y metodológicos distintos. El enfoque cualitativo, en particular, se centra en comprender los fenómenos sociales desde la perspectiva de los participantes, en contraste con la perspectiva del investigador. En el enfoque cualitativo, los datos tienden a ser descriptivos y subjetivos, y la interpretación de los datos es un proceso continuo y reflexivo

3.2. Diseño de Investigación

Se debe señalar que un diseño de investigación es sobre la investigación que se pretende realizar. Hernández (2020) señala que:

La investigación no experimental se caracteriza por no manipular deliberadamente las variables independientes. En este tipo de investigación, se observan los fenómenos tal y como ocurren en su contexto natural y luego se analizan. En el caso de esta investigación, se considera no experimental, ya que no se observan los procesos actuales con el fin de proponer un diseño que solucione el problema sin modificar las variables independientes.

Por lo tanto, un diseño de investigación se refiere al proceso que se llevará a cabo para recopilar información y abordar los objetivos planteados. Este diseño se establece de manera explícita, definiendo los pasos a seguir.

3.2.1. Diseño no experimental

La presente investigación adoptará un diseño no experimental, el cual se basará en el análisis, descripción y observación de la información obtenida, sin realizar modificaciones significativas en las variables. Esto nos permitirá visualizar e interpretar los datos recopilados mediante el instrumento utilizado en la investigación, con el objetivo de establecer conclusiones y recomendaciones relevantes.

Según Fraenkel y Wallen (2006), un diseño no experimental implica la observación y medición de variables, pero no implica una manipulación deliberada de las mismas. En otras palabras, los investigadores no controlan directamente las variables independientes, simplemente las observan y miden en un contexto natural o no manipulado. Es importante destacar que el diseño no experimental no permite establecer relaciones causales entre variables, ya que no hay una manipulación activa de las mismas.

3.3. Nivel de la investigación

3.3.1. Investigación Exploratoria

Según Creswell (2014), la investigación exploratoria se emplea para examinar a fondo un tema o problema de investigación con el propósito de generar ideas y obtener una mejor comprensión del fenómeno en cuestión. A través de la investigación exploratoria, podemos formular hipótesis que nos ayudarán a comprender de manera más precisa el fenómeno que estamos estudiando, lo que nos permitirá llevar a cabo un estudio riguroso y específico.

Adicionalmente, Moustakas (1994) menciona que la investigación exploratoria resulta especialmente útil en la etapa inicial de un proyecto de investigación, cuando el investigador busca comprender un fenómeno o problema de investigación. La investigación exploratoria puede contribuir a definir y enfocar el problema de investigación. Por tanto, esta herramienta es ampliamente utilizada para planificar y diseñar la investigación, con el objetivo de mejorar la calidad y eficacia del trabajo.

3.4. Tipo de investigación

3.4.1. Investigación bibliográfica

El proceso de investigación bibliográfica en el presente estudio implica la recopilación de diversos conceptos con el objetivo de obtener un conocimiento sistematizado. Este tipo de indagación respalda la investigación en curso, evitando la duplicación de conocimientos previamente investigados. En relación a la investigación cualitativa, Pérez (2004) señala que la

investigación bibliográfica desempeña un papel fundamental en la definición del problema, así como en la aplicación de técnicas cualitativas como los grupos focales, cuyos resultados se convierten en un "documento" que contiene una gran cantidad de información similar a una biblioteca no catalogada.

De esta forma, se puede inferir que una investigación cualitativa ofrece la posibilidad de obtener información variada y altamente relevante. Para lograrlo, se lleva a cabo una investigación bibliográfica en artículos, revistas e internet, seguida del análisis de toda la información recopilada durante el transcurso de la investigación.

3.5. Modalidad de la investigación

3.5.1. Modalidad de la propuesta tecnológica

Según el Reglamento de Régimen Académico (RRA, 2017) del Consejo de Educación Superior, se reconoce la modalidad de Propuesta Tecnológica como uno de los trabajos de grado en carreras de formación técnica superior, tecnológica superior y sus equivalentes, así como en la formación de nivel superior de grado. Esta modalidad se refiere a la elaboración de una propuesta original o inédita que contribuya a resolver un problema profesional dentro de los núcleos problémicos de la carrera.

En este contexto, el presente proyecto se enfoca en la "Actualización y mantenimiento de la página web de la Carrera de Pedagogía de las Ciencias Experimentales Informática", el cual se desarrollará siguiendo los lineamientos establecidos por los organismos institucionales. Este proyecto se enmarca en la Modalidad Propuesta Tecnológica y tiene como objetivo la mejora y mantenimiento de la página web de la mencionada carrera.

3.6. Descripción de la propuesta

El análisis de riesgos informáticos es un proceso utilizado para identificar, evaluar y priorizar los posibles riesgos que pueden afectar la seguridad de los sistemas de información y tecnología en una organización. Consiste en analizar tanto las amenazas potenciales como las vulnerabilidades existentes, y determinar la probabilidad de que ocurran eventos adversos y el impacto que podrían tener en los activos de información y en las operaciones del negocio.

Durante el análisis de riesgos informáticos, se realiza una evaluación exhaustiva de los activos de valor, como datos sensibles, infraestructura tecnológica, aplicaciones y sistemas. Se identifican las amenazas potenciales, como ataques cibernéticos, malware, accesos no autorizados o desastres naturales, y se evalúa la vulnerabilidad de los activos ante estas amenazas. A partir de esta evaluación, se determina la probabilidad de que ocurran eventos adversos y se estima el impacto que podrían tener en términos de pérdida financiera, daño a la reputación, interrupción de operaciones o violación de la privacidad basado en MAGERIT.

Con base en los resultados del análisis, se priorizan los riesgos identificados y se desarrollan estrategias de mitigación y planes de respuesta. Estas estrategias pueden incluir medidas de seguridad, como la implementación de controles técnicos, la capacitación del personal, la creación de políticas y procedimientos de seguridad, y la realización de pruebas y auditorías periódicas.

3.7. Población y muestra

Según Arias (2006), la población se define como "un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación" (p. 81). En el proyecto en cuestión, se recopila información de un profesor de la universidad como parte de la población de estudio, la cual será posteriormente analizada e interpretada con el objetivo de determinar si el análisis de riesgos es beneficioso para la seguridad de la información.

3.8. Muestreo no probabilístico

Según un estudio realizado por Argibay (2009), el muestreo no probabilístico se utiliza cuando se tiene acceso limitado a la población de estudio o cuando no es posible identificar una muestra representativa. Además, el muestreo no probabilístico puede ser una opción adecuada en investigaciones exploratorias. Es importante tener en cuenta que los resultados obtenidos a través de este tipo de muestreo no pueden generalizarse a toda la población,

debido a que la selección no es aleatoria y puede presentar sesgos. Por lo tanto, es fundamental que los investigadores reconozcan las limitaciones del muestreo no probabilístico.

3.9. Técnica e instrumentos

Según Eco (1999), la selección de la técnica y los instrumentos de investigación se basa en el problema de investigación y los objetivos del estudio. Los instrumentos de investigación pueden incluir cuestionarios, entrevistas, pruebas, observaciones u otros métodos que permitan obtener información sobre el fenómeno en estudio. Es importante asegurarse de que los instrumentos sean válidos y confiables, además de adaptarse al contexto cultural y lingüístico de la población de estudio, para garantizar la precisión de los resultados del proceso de investigación

3.10. Método de análisis de riesgos (MAGERIT)

Existen varios marcos regulatorios para realizar una evaluación y gestión de riesgos, en este caso en particular se utiliza MAGERIT, a continuación, se detalla una lista de pasos para ejecutar un análisis de riesgos acorde al Ministerio de Hacienda y Administraciones Públicas (2012).

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
5. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

3.10.1. Activos

Acorde al Ministerio de Hacienda y Administraciones Públicas (2012) para una organización los activos son la información que maneja la empresa, el hardware que hace posible el desarrollo de todos los procesos del negocio, las personas encargadas de participar en todos los procesos y todo esto que se menciona es susceptible de ser vulnerado ya sea de forma accidental o deliberada, en un sistema de información hay 2 cosas esenciales la información que maneja y los servicios que presta.

Dependencias

Acorde Ministerio de Hacienda y Administraciones Públicas (2012) hay dos elementos esenciales información y servicios, pero él árbol de dependencias se construye de activos más básicos que forman parte de la empresa como: equipos, comunicaciones, instalaciones y personas que trabajan con ellos. Los activos forman árboles o grafos de dependencias donde la seguridad de los activos superiores depende de los activos inferiores, y la propagación del daño se produce de abajo hacia arriba.

Valoración

Según el Ministerio de Hacienda y Administraciones Públicas (2012) la valoración de un activo responde a la siguiente pregunta ¿Por qué interesa un activo? Y para poder responder a la pregunta se debe hacer un análisis desde la perspectiva de “proteger” ya que mientras mayor sea la importancia de dicho activo para mantener la continuidad de negocio de la empresa mayor nivel de protección requiere.

Dimensiones

El Ministerio de Hacienda y Administraciones Públicas (2012) afirma que entender la dimensión o tener una comprensión completa de todos los aspectos relevantes que están

involucrados en una situación determinada es necesario para desarrollar una acción de contingencia adecuada, En ciertos servicios usualmente utilizados por la sociedad de la información como la administración o el comercio electrónicos es fundamental comprender quiénes son los actores involucrados para poder prestar el servicio correctamente y poder identificar y abordar los fallos, tanto accidentales como deliberados, que pudieran ocurrir.

3.10.2. Amenazas

Se clasifican acorde al Ministerio de Hacienda y Administraciones Públicas (2012) en:

- De origen natural
- Del entorno
- Defectos de las aplicaciones
- Causadas por las personas de forma accidental
- Causadas por las personas de forma deliberada

3.10.3. Salvaguardas

De acuerdo con la metodología de análisis y gestión de riesgos de los sistemas de información MAGERIT, propuesta por el Ministerio de Hacienda y Administraciones Públicas, durante los primeros pasos del análisis de riesgos se evalúan los posibles impactos y riesgos que afectarían a los activos sin considerar las salvaguardas implementadas. Esta aproximación permite conocer la situación más crítica en caso de que se retiren dichas salvaguardas. Las salvaguardas se definen como procedimientos o mecanismos tecnológicos que ayudan a reducir el riesgo y pueden ser organizativas, técnicas, físicas o de políticas de personal, dependiendo del tipo de amenaza (Ministerio de Hacienda y Administraciones Públicas, 2012).

3.10.4. Impacto Residual

De acuerdo con la metodología MAGERIT, cuando se implementan ciertas salvaguardas en un sistema de información, éste queda en una situación de posible impacto

residual, la cual se refiere al nivel de impacto que puede ser sufrido por el sistema después de que se han aplicado las salvaguardas. El impacto residual se puede calcular considerando la eficacia de las salvaguardas y se puede acumular sobre los activos inferiores o repercutir sobre los activos superiores. Para calcular el impacto residual, se debe realizar el cálculo de impacto de los activos teniendo en cuenta la nueva magnitud de la degradación después de aplicar las salvaguardas. La magnitud de la degradación se calcula como la proporción que resta entre la eficacia perfecta y la eficacia real de las salvaguardas implementadas (Ministerio de Hacienda y Administraciones Públicas, 2012).

3.10.5. Riesgo Residual

De acuerdo con la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información del Ministerio de Hacienda y Administraciones Públicas (2012), el conjunto de salvaguardas implementadas y la madurez del proceso de gestión determinan el nivel de riesgo residual de un sistema. Este se refiere a la situación de posible impacto después de la implementación de medidas de protección. Para calcular el riesgo residual, se debe tomar en cuenta la magnitud de la degradación y la probabilidad de las amenazas, y repetir los cálculos usando el impacto y la probabilidad residuales de ocurrencia. La magnitud de la degradación se incluye en el cálculo del impacto residual, mientras que la magnitud de la probabilidad residual se calcula restando la eficacia real de las salvaguardas de la eficacia perfecta. El riesgo residual puede ser calculado acumulativamente sobre los activos inferiores o repercutido sobre los activos superiores.

3.11. Limitaciones de la investigación

Esta investigación presentó varias limitaciones importantes. En primer lugar, la cantidad reducida de participantes fue una limitación significativa. Al tener solamente un participante en la entrevista, resulta difícil generalizar los resultados obtenidos, ya que no podemos afirmar que

las experiencias y opiniones de dicho participante sean representativas de la población en general.

Otra limitación a tener en cuenta es la posibilidad de sesgos en la información proporcionada por el participante. Aunque se realizaron preguntas abiertas y neutrales, existe la posibilidad de que el participante haya sido influenciado por su propio punto de vista o por factores externos que no se detectaron durante la entrevista.

Además, es importante destacar que la entrevista se llevó a cabo en un único momento en el tiempo, lo cual impide asegurar que las respuestas del participante reflejen su opinión a largo plazo. Además, al tratarse de una sola entrevista, se limita la capacidad de profundizar en ciertos temas y explorar diferentes perspectivas.

Por último, es fundamental tener en cuenta que esta investigación se realizó en un contexto específico, por lo que los resultados pueden no ser generalizables a otras organizaciones o situaciones. Por lo tanto, se recomienda interpretar los resultados con precaución y considerarlos como una contribución para comprender el tema en cuestión, en lugar de considerarlos como una conclusión definitiva.

CAPÍTULO IV: IMPLEMENTACIÓN

4. Formalización de las actividades

Acorde al Ministerio de Hacienda y Administraciones Públicas (2012) la formalización consiste en un conjunto de actividades que permiten desarrollar el análisis de riesgo, las cuales se detallan a continuación:

- Identificar y valorar activos
- Identificar y valorar amenazas
- Situación actual de salvaguardas
- Estado de riesgo

4.1. Tarea MAR 1: Caracterización de los activos

Para realizar un análisis de riesgo es necesario establecer una situación actual del área que se busca analizar, Acorde al Ministerio de Hacienda y Administraciones Públicas (2012) la caracterización de los activos es un proceso necesario para determinar donde estén ubicados los activos que se consideren importantes con su respectiva valoración para la empresa. La valoración consiste en asignar al activo un numero entre 1 y 5, siendo 1 el valor donde el riesgo impacta menos y 5 el valor donde el riesgo impacta más en las actividades a desarrollar en la empresa

Tabla 1.

Caracterización de los activos

Activo	Descripción	Ubicación Física	Valoración (1-5)	Dimensión	Coste de impacto
Switches	Dispositivos de red para interconectar equipos en la red local.	Salas de red	3	Confidencialidad (B) Integridad (A) Disponibilidad (A)	Interrupción de servicio Pérdida de productividad
Routers	Dispositivos de red para dirigir el tráfico entre redes.	Salas de red	4	Confidencialidad (B) Integridad (A) Disponibilidad (A)	Interrupción de servicio Pérdida de productividad
Estaciones de trabajo UGT	Equipos de escritorio para los especialistas encargados del maneja y administración del sistema informático de la empresa.	Oficinas	4	Confidencialidad (M) Integridad (M) Disponibilidad (M)	Pérdida de datos Tiempo de inactividad Pérdida de productividad
Servidor de gestión de usuarios	Dispositivo encargado de asignar roles a los usuarios para la organización, permitiendo así que estos manipulen los datos.	Sala de servidores	5	Confidencialidad (A) Integridad (A) Disponibilidad (A)	Vulneración de datos Tiempo de inactividad Pérdida de confianza del cliente
Servidor de correos	Dispositivo encargado de la administración de los correos de todos los empleados.	Sala de servidores	5	Confidencialidad (A) Integridad (A) Disponibilidad (A)	Vulneración de datos Tiempo de inactividad Pérdida de confianza del cliente

Nota. Tabla donde se detallan los activos pertenecientes a la vlan.

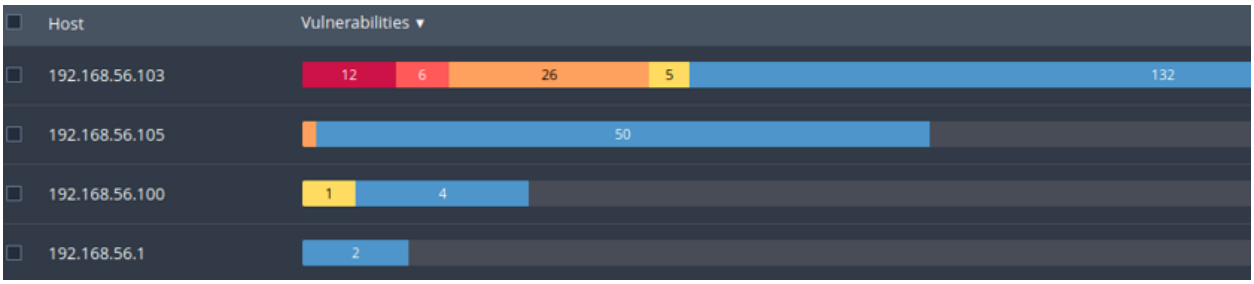
4.2. Tarea MAR 2: Caracterización de las amenazas

Acorde al Ministerio de Hacienda y Administraciones Públicas (2012) el objetivo de esta tarea consiste en dar a conocer el medio al cual se enfrentan los activos, los posibles sucesos de que se ejecute un ataque, las consecuencias, y su probabilidad.

4.2.1. Escaneo de vulnerabilidades con Nessus

Acorde a KeepCoding (2023) Nessus es un software para ciberseguridad, tanto open source como de pago, el cual escanea vulnerabilidades de distintos sistemas operativos. Para caracterizar las amenazas a las que se pueda enfrentar el servidor de la Unidad de Gestión Tecnológica se hará uso de la herramienta de escaneo de vulnerabilidades y con los resultados obtenidos se determinara el nivel de riesgo.

Al aplicar el escaneo básico de red de Nessus se identifican la IP de los dispositivos y las posibles vulnerabilidades. Se puede delimitar los activos a ser escaneados si se conoce su direccionamiento IP.



Con los resultados obtenidos se puede determinar que el dispositivo con dirección IP 192.168.56.103 el cual en este caso es el Servidor de correos presenta una alarmante cifra de vulnerabilidades que vienen clasificados por un código de color y un puntaje.

Tabla 2.

Vulnerabilidades encontradas mediante escaneo básico de red

Severidad	CVSS	Nombre	Familia	Cant
Critical	10	NFS Exported Share Information Disclosure	RPC	1
Critical	10	Rexecd Service Detection	Service Detection	1
Critical	10	Unix Operating System Unsupported	General	1
Critical	10	VNC Server 'password' Password	Gain a Shell remotly	1
Critical	9.8	Bind Shell Backdoor Detection	Backdoors	1
Critical	10	SSL (multiple issues)	Gain a Shell remotly	3
High	7.5	NFS Shares World Readable	RPC	1
High	7.5	rlogin Service Detection	Service Detection	1
High	7.5	Samba Badlock Vulnerability	General	1
Medium	6.5	TLS Version 1.0 Protocol Detection	Service detection	2
Medium	6.5	Unencrypted Telnet Server	Misc.	1
Medium	5.9	SSL DROWN Attack Vulnerability	Misc.	1
LOW	2.6	X server Detection	Service Detection	1

Nota. Principales vulnerabilidades tomadas en cuenta para efectuar los demás procesos.

4.2.2. Categorización de amenazas

Tabla 3.

Posibles amenazas a las que se enfrente el sistema

Amenaza	Descripción	Probabilidad	Impacto	Categoría
Ataque de malware	Infección de sistemas por software infeccioso.	Alta	Medio	Amenazas de seguridad cibernética
Incendios	Fuegos en las instalaciones que	Baja	Alto	Amenaza Física

	afecta la infraestructura.			
Error humano	Acciones involuntarias o negligencias de los usuarios.	Media	Medio	Amenazas internas
Fallo de suministro eléctrico	Interrupción del suministro eléctrico que afecta la disponibilidad del servicio.	Media	Alto	Amenazas externas
Grupos Mal intencionados	Grupos de personas con conocimientos técnicos necesarios para generar un ataque al sistema.	Media	Alto	Amenazas de seguridad cibernética
Conducta deshonesta del personal	Acciones o comportamientos por parte de un empleado que involucran engaño, falta de ética o violación de normas y políticas establecidas en el entorno laboral.	Alta	Alto	Amenazas Internas

Nota. Las amenazas pueden ser de carácter interno y externo a la empresa.

4.2.3. Mapa de riesgos

Tabla 4.

Desarrollo del mapa de riesgos para el sistema

Activo	Amenaza	Vulnerabilidad	Impacto	Riesgo
Servidor de correos	Acceso no autorizado Ataque DDoS Ataque de malware Fallo del enlace de red	Servicios y protocolos inseguros Aplicaciones web vulnerables Bases de datos con configuraciones inseguras Servicios de red inseguros Vulnerabilidades de sistema operativo	Interrupción del servicio o continuidad del negocio.	Alto
Estaciones de trabajo UGT	Acceso no autorizado Ataque de malware Fallo del enlace de red	Aplicaciones web vulnerables Servicios de red inseguros Vulnerabilidades de sistema operativo	Interrupción del servicio o continuidad del negocio.	Alto

4.3. Tarea MAR 3: Caracterización de las salvaguardas

Acorde al Ministerio de Hacienda y Administraciones Públicas (2012) el fin de este proceso es considerar que requiere para proteger la continuidad del negocio y saber si se tiene protección a la altura de las necesidades.

4.3.1. Identificación Salvaguardas

Tabla 5.

Salvaguardas propuestas para los activos

Vulnerabilidad	Salvaguarda propuesta
Servidor FTP con credenciales débiles o anónimas	Implementación de autenticación segura y fuertes políticas de contraseñas en el servidor FTP.
Servidor Telnet sin autenticación o con contraseñas débiles	Desactivar el servicio Telnet y utilizar protocolos de acceso remoto seguros como SSH. Implementar políticas de contraseñas fuertes.
Servidor SSH con contraseñas fáciles de adivinar	Utilizar autenticación de clave pública en lugar de contraseñas. Deshabilitar la autenticación basada en contraseñas.
Servidor SNMP con cadena de comunidad predeterminada o débil	Cambiar la cadena de comunidad predeterminada y utilizar una cadena fuerte. Restringir el acceso SNMP solo a sistemas autorizados.
Servidores DNS mal configurados o vulnerables a ataques de envenenamiento	Configurar el servidor DNS de manera segura, implementar DNSSEC para autenticación de registros y realizar auditorías periódicas.
Fallos de seguridad conocidos en el sistema operativo	Mantener actualizado el sistema operativo con los últimos parches de seguridad. Configurar cortafuegos y utilizar herramientas de detección de intrusiones.

4.4. Tarea MAR 4: Estimación del estado de riesgo

Acorde al Ministerio de Hacienda y Administraciones Públicas (2012) el fin de este proceso consiste en considerar que requiere para proteger la continuidad del negocio y saber si se tiene protección a la altura de las necesidades del caso, para ello se utilizan las siguientes rúbricas: MB: muy bajo, B: bajo, M: medio, A: alto, MA: muy alto.

4.4.1. Estimación del Impacto

Tabla 6.

Impacto estimado en los activos

Activo	Valor del Activo	Magnitud del Impacto	Magnitud del riesgo
Switches	M	B	M
Routers	A	A	MA
Estaciones de trabajo	B	M	M
Servidor de usuarios	A	A	MA
Servidor de correos	A	B	A

4.4.2. Estimación del riesgo

Tabla 7.

Riesgo estimado en los activos

Activo	Valor del Activo	Magnitud del Impacto Residual	Magnitud de la Probabilidad	Magnitud del riesgo
Switches	M	B	B	M
Routers	A	B	A	MA
Estaciones de trabajo	B	B	M	B
Servidor de usuarios	A	MA	A	MA
Servidor de correos	A	B	B	B

4.5. Resultados

En el proceso de evaluación de riesgos utilizando la metodología MAGERIT, se ha llevado a cabo un análisis detallado de los activos de la organización y se han identificado las amenazas, vulnerabilidades y salvaguardas asociadas. A través de la estimación del impacto potencial y residual, así como la valoración del riesgo, hemos obtenido una visión general de la seguridad de los activos evaluados.

Al analizar los resultados obtenidos, podemos destacar varios aspectos significativos. En primer lugar, el servidor de correos es un activo demasiado vulnerable y debe ponerse en práctica la implementación de las salvaguardas para poder reducir el riesgo.

Por otro lado, se propusieron una serie de salvaguardas para mitigar los riesgos identificados. Estas medidas incluyen la implementación de autenticación segura, políticas de contraseñas fuertes, desactivación de servicios no seguros, configuración segura de servidores y actualizaciones regulares del sistema operativo. Y con ello contribuyen a reducir el impacto residual y el riesgo asociado a los activos evaluados.

Sin embargo, es importante destacar que la estimación del riesgo y la implementación de salvaguardas son procesos continuos y deben ser revisados y actualizados regularmente. Las vulnerabilidades suelen estar presentes en cualquier sistema que tenga información, por lo que es esencial mantenerse al día con las últimas prácticas de seguridad y adaptar las medidas de protección en consecuencia.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- El escaneo de vulnerabilidades realizado ha sido fundamental para obtener información detallada sobre el estado de seguridad del servidor de la red, se han identificado y evaluado las posibles vulnerabilidades presentes en el sistema. Con ello se determinó que el nivel de riesgo era alto debido a deficientes configuraciones en el servidor de correos, Esto ha permitido una visión clara de las debilidades existentes y ha brindado una base sólida para la toma de decisiones en materia de seguridad.
- Nessus al momento de realizar un escaneo básico de la red, encuentra vulnerabilidades y les asigna una métrica acorde a CVSS, proporcionando una base para evaluar la gravedad y el impacto potencial de las vulnerabilidades identificadas en el servidor de correos. El uso de CVSS permite una clasificación objetiva de las amenazas y ayuda a priorizar las acciones de mitigación según su importancia relativa. Esto brinda una estructura sólida para la gestión de riesgos y la asignación de recursos en función de la criticidad de cada vulnerabilidad.
- Mediante las tareas MAR de la metodología MAGERIT se pudo formalizar los procesos para un futuro plan de gestión del riesgo. Al presentar las tablas donde están los activos, el valor que tienen para la continuidad del negocio y el impacto que tendrían de verse vulnerados en algún instante, se resalta la importancia de invertir en la seguridad de la información. Esta exposición puede ser utilizada para respaldar la toma de decisiones estratégicas, obtener el apoyo de la alta dirección y promover la implementación de medidas de seguridad adecuadas.

Recomendaciones

- En futuras investigaciones, se recomienda ampliar el alcance del análisis de riesgos a otros activos de la organización, además de los mencionados anteriormente. Esto permitirá tener una visión más completa de la seguridad de la infraestructura y los sistemas de información, identificando posibles puntos débiles y áreas de mejora adicionales.
- Como complemento al escaneo de vulnerabilidades, se sugiere realizar pruebas de penetración en los sistemas y redes de la organización. Estas pruebas permiten evaluar de manera más exhaustiva la resistencia de los sistemas ante ataques reales, identificar posibles brechas de seguridad y validar la efectividad de las medidas de protección implementadas.
- La ciberseguridad es un campo en constante evolución, con nuevas amenazas y vulnerabilidades que surgen regularmente. Por lo tanto, se recomienda mantenerse actualizado sobre las últimas tendencias, ataques y medidas de seguridad. Esto puede lograrse mediante la participación en comunidades de seguridad, la asistencia a conferencias y la lectura de publicaciones especializadas. Estar al tanto de las últimas amenazas permitirá adaptar las estrategias de seguridad y tomar medidas preventivas para proteger mejor los activos de la organización.

BIBLIOGRAFÍA

Altube, R. (2021, 5 de noviembre). Kali Linux: qué es y características principales. OpenWebinars. https://openwebinars.net/blog/kali-linux-que-es-y-caracteristicas-principales/

Ambit BST. (2020, 7 de mayo). Análisis de riesgos informáticos y ciberseguridad. Recuperado el 17 de abril de 2023, de https://www.ambit-bst.com/blog/an%C3%A1lisis-de-riesgos-inform%C3%A1ticos-y-ciberseguridad

Aria. (2006). *El Proyecto de Investigación. Introducción a la Metodología Científica. 6ta. Edición*. Google Books.

https://books.google.com.ec/books?id=W5n0BgAAQBAJ

Argibay, J. C., (2009). MUESTRA EN INVESTIGACION CUANTITATIVA. Subjetividad y Procesos Cognitivos, 13(1), 13-29.

Cloudflare. (s. f.). Open Systems Interconnection Model (OSI). Recuperado 23 de marzo de 2023, de https://www.cloudflare.com/es-es/learning/ddos/glossary/open-systems-interconnection-model-osi/

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

De Luz, S. (11 de enero de 2023). VLAN: tipos y configuración. Recuperado el 22 de marzo de 2023, de https://www.redeszone.net/tutoriales/redes-cable/vlan-tipos-configuracion/

FIRST.Org. (2019). Common Vulnerability Scoring System v3.1: Specification Document. Recuperado el 30 de marzo de 2023, de https://www.first.org/cvss/v3.1/specification-document

Fraenkel, J. R. & Wallen, N. E. (2006). How to design and evaluate research in education. New York: McGraw-Hill.

Gamboa Suarez, J. L. (2020). Importancia de la seguridad informática y ciberseguridad en el mundo actual.

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. Mcgraw-hill.

IDRIC. (2022, 3 de junio). Beneficios de llevar a cabo un análisis de vulnerabilidades. IDRIC. https://www.idric.com.mx/blog/post/beneficios-de-llevar-cabo-un-analisis-de-vulnerabilidades

KeepCoding. (2023, 12 de enero). ¿Qué es Nessus? Recuperado de https://keepcoding.io/blog/que-es-nessus/

Mustakas, C. (1994). *Métodos de investigación fenomenológica* . Publicaciones SAGE, Inc., https://dx.doiorg/10.4135/9781412995658

Profesional Review. (2018, 22 de noviembre). ¿Qué es el modelo OSI y para qué se utiliza? Recuperado el 16 de abril de 2023, de https://www.profesionalreview.com/2018/11/22/modelo-osi/

Ministerio de Hacienda y Administraciones Públicas. (2012). Metodología de Análisis y Gestión

de Riesgos de los Sistemas de Información. https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

OStec Blog. (2021, 19 de enero). ¿Qué es el análisis de vulnerabilidades? [Página web]. Recuperado el 30 de marzo de 2023, de https://ostec.blog/es/aprendizaje-descubrimiento/que-es-el-analisis-de-vulnerabilidades/

Krypton Solid. (s.f.). ¿Qué es CVSS? Common Vulnerability Scoring System. Recuperado el 4 de marzo de 2023, de https://kryptonsolid.com/que-es-cvss-common-vulnerability-scoring-system/

Reglamento de Régimen Académico. (2017). www.ces.gob.ec. Recuperado 22 de febrero de 2023, de https://www.ces.gob.ec/lotaip/2017/Diciembre/Anexos+Procu/An-lit-a2-Reglamento+de+R%C3%A9gimen+Acad%C3%A9mico.pdf

Serrano Vazquez, L. M. (2020). Guía de buenas prácticas de seguridad en redes para la configuración de dispositivos de capa 2 y 3 del modelo OSI y validación en una red de prueba (Tesis de licenciatura). Universidad del Azuay.

WeLiveSecurity. (4 de agosto de 2014). Vulnerabilidades: ¿qué es CVSS y cómo utilizarlo? [Entrada de blog]. Recuperado el 19 de marzo de 2023, de https://www.welivesecurity.com/la-es/2014/08/04/vulnerabilidades-que-es-cvss-como-utilizarlo/

ANEXOS

Anexo A: Adjuntar anexos si los necesita para la elaboración de la tesis

1.1. Desarrollo de la entrevista

Como parte de la investigación cualitativa el método de la entrevista es ideal para obtener un punto de vista sobre la realidad actual de la seguridad de los sistemas de información permitiendo así obtener una comprensión más amplia de la importancia del tema a tratar.

1.1.1. ¿Cuáles son los principales desafíos que enfrenta la ciberseguridad en la actualidad y cómo se pueden abordar?

Los principales desafíos que enfrenta la ciberseguridad en la actualidad, son la constante evolución de los ataques, las amenazas persistentes avanzadas, el incremento de ataques a nivel mundial debido a ransomware, desatención en la actualización de los sistemas computacionales y la falta de capacitación, desconocimiento y concientización sobre las consecuencias a las que las organizaciones se enfrentan cuando se presentan ataques, extorción, robo de información, desprestigio, etc. debido a una inadecuada aplicación de mecanismos y herramientas que permiten incrementar la seguridad de la información.

1.1.2. ¿Cómo se pueden identificar las amenazas y vulnerabilidades en los sistemas de información y redes de una organización y qué medidas de protección se deben implementar?

Para identificar amenazas y vulnerabilidades en los sistemas de información se deben utilizar métodos y herramientas avanzadas de “análisis de vulnerabilidades” que permitan obtener información detallada sobre su nivel de actualización y mejora sobre la seguridad de cada uno de ellos. Se deben utilizar varias herramientas de análisis y contrastar los resultados

obtenidos para ampliar el rango de conocimiento de la desactualización que puedan tener los sistemas. Una vez que se hayan obtenido y contrastados los resultados, inmediatamente se deben aplicar las recomendaciones que estas mismas herramientas le presentan a los responsables de las áreas de seguridad y tecnologías de la información y comunicación, para con ello elevar los niveles de protección de seguridad a la infraestructura tecnológica de las organizaciones.

1.1.3. ¿Cuál es la importancia de la educación y la concientización en materia de ciberseguridad para las empresas y organizaciones?

La educación y concientización juegan un papel muy importante en las organizaciones. Este un reto al que la alta dirección y gerencia debe enfocar sus esfuerzos para tener personal y colaboradores altamente capacitados sobre la importancia y consecuencias que se pueden presentar con la información que manejan y producen. Un personal capacitado hace que la información de la empresa este seguro, pero ayudada con la aplicación de estandartes y herramientas de seguridad de la información.

1.1.4. ¿Cómo se puede evaluar la efectividad de un plan de seguridad de la información y qué factores son importantes a considerar en esta evaluación?

Para evaluar la efectividad de un plan de seguridad de la información primero se deben aplicar estándares enfocados a elevar el nivel de ciberseguridad y con la implementación de un adecuado sistema de gestión de seguridad de la información que permitan a la organización identificar cuáles son sus infraestructuras críticas, realizar la administración de activos y sobre todo gestión de riesgos de los mismos. Una vez realizada esta tarea se aplican controles y políticas que permitirán evaluar de manera continua los niveles de seguridad implementados. Este proceso debe ser activo y continúo aplicando el ciclo de Deming de planificar, hacer, revisar y actuar.

1.1.5. ¿Cómo se pueden diseñar y desarrollar políticas de seguridad de la información que sean efectivas y se ajusten a las necesidades de una organización?

La alta gerencia es la principal promotora de elevar los niveles de seguridad de la información con el apoyo del área de tecnologías de la información y comunicación. De la implantación de un sistema de gestión de seguridad de la información se empiezan a desprender automáticamente los controles y políticas a aplicar, que se adaptan a la realidad empresarial.

Con base en las respuestas obtenidas se puede llegar a la siguiente conclusión que los análisis de vulnerabilidades permiten a las empresas de cada país realizar un monitoreo sobre la situación actual de la seguridad de la información que manejan de clientes u otras entidades y estos son uno de varios pasos importantes necesarios para realizar planes de mejora de la empresa en cuanto a seguridad de la información se refiere.