



UNIVERSIDAD DE MARGARITA
SUBSISTEMA DE DOCENCIA
DECANATO DE INGENIERÍA Y AFINES
COORDINACIÓN DE INVESTIGACIÓN Y PASANTÍA

**AUDITORÍA DE RED PARA LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN
EN LA FRANQUICIA INMOBILIARIA RE/MAX 2MIL C.A. ESTADO NUEVA ESPARTA**

Elaborado por: Br. Domingo Suarez

Tutor: Prof. MSc. Emmanuel Caraballo

El Valle del Espíritu Santo, junio de 2023

DEDICATORIA

Con gran emoción y agradecimiento, dedico este trabajo de investigación a aquellos que nos brindan amor, apoyo y compañía en mi vida: mi familia, mis amigos y mis seres queridos. Por su incondicional amor y respaldo en cada paso que damos. Por ser mi refugio en los momentos difíciles y por celebrar en los momentos de alegría, su amor y apoyo son la base de mi fortaleza. A todos aquellos que, con su presencia y cariño, han dejado una huella imborrable en mi vida. A aquellos que nos han brindado palabras de aliento, consejos sabios y un hombro en el cual apoyarnos para convertirnos en la persona que somos hoy, sin su apoyo incondicional, este logro no hubiera sido posible.

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento a mi tutor, el Prof. MSc. Emmanuel Caraballo, por su invaluable ayuda y orientación en el desarrollo de esta investigación. Su dedicación, paciencia y apoyo fueron fundamentales para que pudiera culminar este proyecto de manera exitosa. También quiero reconocer el esfuerzo y la disposición de las Profesoras Yemnel Torcat, Nelly Cumaraima, Isis Rueda y Ana Blanco, quienes amablemente me brindaron su tiempo y conocimientos para responder a todas mis consultas y dudas. Su valiosa colaboración permitió enriquecer y profundizar en el tema de investigación.

Por otro lado, no puedo dejar de mencionar a mi familia que siempre me ha apoyado, a mis Bois; a mi hermano de otra madre, José López (Pelox) por quedarse hasta las madrugadas en Discord, (a mis compañeros de estudio también), mis amigos de la comunidad online, y al Prof. Flavio Rosales, quien sin saberlo fue un gran motivador indirecto del tema seleccionado. Su interés y pasión por el campo de estudio despertó en mí la curiosidad y el entusiasmo para investigar más en profundidad sobre el tema. En definitiva, quiero expresar mi profundo agradecimiento a todas estas personas que hicieron posible este proyecto de investigación, y cuyos aportes fueron determinantes para lograr un trabajo riguroso y de calidad.

INDICE

DEDICATORIA	i
AGRADECIMIENTOS	ii
LISTA DE GRÁFICOS.....	v
LISTA DE TABLAS.....	vi
LISTA DE FIGURAS.....	vii
RESUMEN.....	viii
INTRODUCCIÓN	1
PARTE I DESCRIPCIÓN GENERAL DEL PROBLEMA	9
1.1 Formulación del Problema	9
1.2 Interrogantes	13
1.3 Objetivo general	14
1.4 Objetivos específicos	14
1.5 Valor Académico de la Investigación.....	14
PARTE II DESCRIPCIÓN TEÓRICA	16
2.1 Antecedentes de Investigación.....	16
2.2. Bases Teóricas.....	18
2.3 Bases legales	26
2.4 Definición de Términos.....	29
PARTE III	32
DESCRIPCIÓN METODOLÓGICA	32
3.1. Naturaleza de la Investigación	32
3.1.1. Tipo de investigación.....	32
3.1.2. Diseño de la investigación.....	33
3.1.3. Población y Muestra	33
3.1.4. Técnicas de Recolección de Datos	34
3.1.4. Técnicas de Análisis de Datos	34
PARTE IV.....	36
ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS.....	36
4.1 Evaluación de las áreas de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A., donde presenta vulnerabilidades.	36

4.2 Identificación del estado actual de la seguridad informática de la franquicia inmobiliaria RE/MAX 2Mil C.A. en relación con el estándar 27000 y 27001 de la International Organization for Standardization (ISO).....	39
4.3 Estrategias de seguridad informática más convenientes para proteger los puntos vulnerables de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A.	50
PARTE V.....	52
PROPUESTA.....	52
5.1 Importancia de la Propuesta.	52
5.2 Viabilidad de aplicación de la Propuesta.	52
5.3 Objetivos de la Propuesta.	54
5.4 Representación gráfica y estructura de la Propuesta.	55
CONCLUSIONES Y RECOMENDACIONES	59
Conclusiones.....	59
Recomendaciones.....	60

LISTA DE GRÁFICOS

- Gráfico 1. Clasificación de riesgos**¡Error! Marcador no definido.**
- Gráfico 2. Topología de red de RE/MAX 2Mil**¡Error! Marcador no definido.**
- Gráfico 3. La inmobiliaria proporciona una red informática **¡Error! Marcador no definido.**
- Gráfico 4. Dispuesto a colaborar y proporcionar acceso a la infraestructura **¡Error! Marcador no definido.**
- Gráfico 5. Importancia de realizar la auditoria en la franquicia..... **¡Error! Marcador no definido.**
- Gráfico 6. Principales desafíos al realizar la auditoria en la franquicia..**¡Error! Marcador no definido.**
- Gráfico 7. Familiarización con las políticas y procedimientos de seguridad..... **¡Error! Marcador no definido.**
- Gráfico 8. Capacitación sobre prácticas de seguridad informática en el entorno laboral**¡Error! Marcador no definido.**
- Gráfico 9. Contraseñas seguras para acceder a los recursos de la compañía **¡Error! Marcador no definido.**
- Gráfico 10. Experimentados intentos de intrusión o actividades sospechosas en la red de la compañía.....**¡Error! Marcador no definido.**
- Gráfico 11. Cumplen regularmente las actualizaciones y parches de seguridad .. **¡Error! Marcador no definido.**

LISTA DE TABLAS

Tabla 1: Herramientas tecnológicas para realizar la propuesta de auditoría.....**¡Error! Marcador no definido.**

Tabla 2: Costo de los instrumentos tecnológicos para ejecutar la propuesta de auditoria**¡Error! Marcador no definido.**

Tabla 3: Inversión de los instrumentos tecnológicos para el correcto uso de la aplicación móvil.**¡Error! Marcador no definido.**

LISTA DE FIGURAS

Figura 1: Aspecto actual de la red de la franquicia inmobiliaria RE/MAX 2Mil.	55
Figura 2: RE/MAX 2Mil en día laboral utilizando la infraestructura de la oficina.	56
Figura 3: Cableado de la oficina RE/MAX 2Mil.	56
Figura 4: Infraestructura recomendada para la franquicia inmobiliaria RE/MAX 2Mil ...	57
Figura 5: Infraestructura recomendada en software Cisco Packet Tracer.....	57
Figura 6: Representación de Infraestructura en software Cisco Packet Tracer	58

UNIVERSIDAD DE MARGARITA
ALMA MATER DEL CARIBE
COORDINACIÓN DE INVESTIGACIÓN

**AUDITORÍA DE RED PARA LOS PROCESOS DE SEGURIDAD DE LA INFORMACIÓN
EN LA FRANQUICIA INMOBILIARIA RE/MAX 2MIL C.A. ESTADO NUEVA ESPARTA**

Autor: Domingo Alejandro Suárez Avendaño

Tutor: Prof. MSc. Emmanuel Caraballo

Julio de 2023

RESUMEN

La auditoría de redes se ha convertido en un requisito internacional como consecuencia de la sofisticación y frecuencia de las ciberamenazas en la actualidad, para garantizar la seguridad de los sistemas informáticos y de comunicación de las empresas, la auditoría de redes es una actividad crucial. Además de certificar el cumplimiento de la legislación y las normas de seguridad, esta actividad ayuda a localizar vulnerabilidades y fallos de seguridad. El presente trabajo descriptivo se encuentra enmarcado dentro de la línea de investigación número 5, “Métodos y Estandarización y de Sistemas”, dentro de su área temática “Auditoría”; a su vez, evalúa de forma crítica el éxito de las precauciones de seguridad actuales y realizar actualizaciones continuas de la seguridad de la red de la franquicia inmobiliaria RE/MAX 2Mil C.A., la auditoría de la red debe ser realizada por personas cualificadas con conocimientos de seguridad informática. En esencia, la auditoría de red es vital para defender los sistemas informáticos de las empresas de las ciberamenazas, involucrando a todas las partes interesadas, los empleados, los gerentes y los proveedores de servicios externos.

Descriptores: gestión de riesgos, respaldo de datos, normativas de seguridad, amenazas cibernéticas, auditoría de red, personal especializado.

INTRODUCCIÓN

Hoy en día, las redes informáticas desempeñan un papel fundamental en el funcionamiento de las empresas de todo el mundo. El acceso a Internet, la interconexión de sistemas, la transferencia de datos y la comunicación en línea son elementos esenciales para el desarrollo de las operaciones empresariales en un entorno cada vez más digitalizado y globalizado. Sin embargo, con la creciente complejidad y sofisticación de las redes, también han surgido nuevos retos y riesgos en términos de seguridad, confidencialidad e integridad de la información. Los ciberataques, las fugas de datos, los errores de configuración y las vulnerabilidades de los sistemas son amenazas latentes que pueden afectar gravemente a las empresas y poner en peligro su reputación, sus operaciones y sus resultados económicos.

En este contexto, se hace imperativo que las empresas realicen auditorías de red periódicas y exhaustivas para evaluar la seguridad y el rendimiento de sus sistemas de información. La auditoría de red es un proceso exhaustivo que implica una revisión detallada de la infraestructura de red, los sistemas, los dispositivos y las políticas de seguridad con el objetivo de identificar posibles vulnerabilidades, detectar anomalías, corregir errores y mejorar la eficiencia operativa. De tal manera, el presente trabajo de investigación pretende analizar la importancia de realizar una auditoría de red en una empresa, teniendo en cuenta la realidad mundial en materia de seguridad de las redes informáticas, se encuentra estructurado de la siguiente manera:

En la Parte I, se realiza la descripción general del problema, donde se detallan los aspectos relacionados al tema objeto de estudio y su justificación, conformado por la formulación del problema, las interrogantes, los objetivos y el valor académico de la investigación.

En la Parte II, se presenta la descripción teórica, donde se desarrollan los principales conceptos asociados a la investigación, constituyéndose en antecedentes, bases teóricas, bases legales y definición de términos.

En la Parte III, se desarrolla la descripción metodológica, donde se expone la naturaleza de la investigación, las técnicas de recolección de datos y las empleadas para analizar dichos datos.

En la **Parte IV**, se presenta el análisis e interpretación de los resultados, donde se analiza cada uno de los objetivos específicos de la investigación en base a los resultados obtenidos; lo que da paso a satisfacer el objetivo general.

En **Conclusiones y Recomendaciones**, se sintetiza, a modo de respuesta, los resultados obtenidos en la investigación, añadiendo sugerencias por parte del investigador para que sean consideradas en estudios posteriores o en implementaciones de proyectos similares.

En **Fuentes Bibliográficas**, se especifica cada uno de los distintos recursos informativos que fueron consultados durante el desarrollo de la investigación; abarcando libros, páginas web, regulaciones legales, documentos digitales, entre otros.

PARTE I

DESCRIPCIÓN GENERAL DEL PROBLEMA

De acuerdo con Arias, F. (2012:41), el planteamiento del problema “consiste en describir de manera amplia la situación objeto de estudio, ubicándola en un contexto que permita comprender su origen, relaciones e incógnitas por responder”. De tal manera, en esta parte I tiene como objeto de estudio realizar la formulación del problema, los objetivos generales y específicos, además, el valor académico que implica esta investigación.

1.1 Formulación del Problema

La auditoría de red es un proceso crítico en las organizaciones a nivel mundial, ya que es necesario garantizar la seguridad y protección de los sistemas informáticos y de comunicación de las empresas, especialmente en el contexto actual de amenazas cibernéticas en constante evolución cada vez más sofisticadas y frecuentes. En 2017, Equifax, una de las tres mayores agencias de información crediticia de Estados Unidos, fue víctima de un ciberataque que expuso los datos personales de 147 millones de consumidores. Una investigación posterior descubrió que el ataque podría haberse evitado si Equifax hubiera realizado una auditoría adecuada de la red y corregido las vulnerabilidades conocidas de sus sistemas. El incidente le costó a la empresa más de 1.400 millones de dólares en multas y honorarios legales. Dos años después, en 2019, el proveedor estadounidense de servicios bancarios y financieros Capital One sufrió un ciberataque que expuso los datos personales de más de 100 millones de clientes. Según una investigación posterior, los atacantes pudieron explotar vulnerabilidades en los cortafuegos de la empresa debido a la falta de auditorías de red adecuadas. El incidente costó a Capital One más de 300 millones de dólares en multas y otros costes.

En 2020, la empresa de software SolarWinds fue víctima de un sofisticado ciberataque que afectó a varias organizaciones gubernamentales y empresariales de Estados Unidos y otros países. El ataque fue desencadenado por una actualización de software malicioso y pasó desapercibido durante meses debido a la falta de auditorías adecuadas de la red.

Según algunos informes, el incidente podría haber costado a las organizaciones afectadas hasta 90.000 millones de dólares en daños y pérdidas. La importancia de la auditoría de red radica en la necesidad de proteger los sistemas de información y de comunicación de la empresa de posibles riesgos de seguridad, como el robo de datos, la pérdida de datos, la interrupción del servicio y el malware.

Los procesos de auditoría de red en dichas organizaciones generalmente implican una revisión exhaustiva de los sistemas y procesos informáticos de la misma, incluyendo la evaluación de los controles de seguridad de la red, la identificación de posibles vulnerabilidades y la recomendación de soluciones para mejorar la seguridad de la red, este es un proceso crucial en las organizaciones a nivel mundial o internacional, ya que ayuda a proteger los sistemas de información, de comunicación de la empresa y a cumplir con las regulaciones tanto como los estándares de seguridad cibernética.

Según Razo, C. (2002), define la auditoría “como la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones”. La auditoría de red incluye la revisión de los controles de seguridad, la evaluación de los sistemas de seguridad y la identificación de posibles vulnerabilidades. Además, la auditoría de red también puede evaluar el rendimiento de la misma, la calidad del servicio y la capacidad de recuperación en caso de posibles fallas. En el contexto empresarial, la auditoría se enfoca en evaluar el desempeño y cumplimiento de los objetivos de la organización. De tal manera Razo, C. (2002) define a la auditoría de red de una empresa como “la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento”.

De otro modo, Alzate, A. (2007), indica que “es importante destacar que la auditoría de red no solo se realiza para detectar posibles fallos o vulnerabilidades en la red, sino también para identificar oportunidades de mejora y optimización del rendimiento de los

sistemas y procesos informáticos de la empresa". No obstante, según Álvarez, L. (2005) "La implementación de políticas y medidas de seguridad informática en las empresas es esencial para proteger la información y garantizar la continuidad del negocio, ya que los ataques cibernéticos pueden causar daños financieros y de reputación significativos". Independientemente de su tamaño o sector, la seguridad informática es un tema de vital importancia para cualquier empresa; es esencial que las mismas aseguren que su red esté protegida contra posibles amenazas. Esto implica no solo la implementación de medidas de seguridad técnica, sino también la capacitación de los empleados y la promoción de una cultura de seguridad informática en toda la organización, ya que representa un aspecto crítico de la gestión empresarial moderna que no puede ser ignorada.

Como indica Bruce, W. (2016), se entiende que el acceso a servicios online ha brindado comodidad a los usuarios, pero a su vez, ha creado una preocupante vulnerabilidad en cuanto a la seguridad de la información personal que se otorga a las empresas, las cuales deben velar por mantener la confidencialidad y resguardo de estos datos ante posibles ataques informáticos. Todo esto trajo mejoras y beneficios, las empresas mejoraron sus servicios, ya que en la actualidad se desarrolla en una etapa digital, donde los servicios son prestados de forma online, de manera que los usuarios no tienen la necesidad de trasladarse a un establecimiento para adquirir un servicio, ahora lo pueden hacer desde la comodidad de su casa. Aunque no todo es bueno, ya que para poder acceder a servicios online se tiene que otorgar una serie de datos e información que se solicitan como requisitos, estos datos quedan bajo el resguardo de la seguridad de la empresa a la que estemos accediendo. Esto es una clara vulnerabilidad, ya que, si la seguridad de la red de la empresa se ve comprometida, los datos de los usuarios pueden quedar en manos de los atacantes.

Así como las personas no tienen que presentarse físicamente a un establecimiento para adquirir un servicio, los atacantes tampoco y pueden atacar la red de una empresa desde cualquier parte del mundo. Una de las modalidades más comunes en ataques a redes de empresas es el denominado ataque de denegación distribuida de servicios o también conocido como DDOS (Distributed Denial of Service), este consiste en saturar la red de una empresa utilizando diferentes medios, de esta manera el atacante pide un

rescate por la información y estabilidad de la red. A su vez, como menciona (Kearns, M. 2004), "Los ataques de denegación distribuida de servicios han sido un método de ataque popular durante muchos años y, en muchos casos, pueden ser extremadamente efectivos, ya que pueden desactivar servicios y sistemas críticos, haciendo que un negocio pierda una gran cantidad de ingresos y dañando su reputación".

De acuerdo con Kshetri, N., & Voas, J. (2017), se logra identificar que a nivel mundial existe una falta de conciencia y preparación en seguridad informática, especialmente en las pequeñas y medianas empresas, las hace más vulnerables a los ataques informáticos y el robo de información sensible de sus clientes. Una gran problemática que existe en la actualidad es el desconocimiento que se tiene sobre estas áreas relacionadas a la seguridad informática, las personas no suelen prestar mucha atención sobre este tema. Las medianas o pequeñas empresas, incluyendo las inmobiliarias, suelen ser más vulnerables a los ataques informáticos debido a que, en general, estas empresas suelen tener menos experiencia en la gestión de la seguridad de la información. En el caso específico de las inmobiliarias, pueden manejar una gran cantidad de información sensible, como nombres completos, números de identificación personal, direcciones, información financiera y otros datos personales. Si esta información cae en manos equivocadas, puede ser utilizada para el robo de identidad, el fraude financiero, el acoso y otros delitos.

Las inmobiliarias también pueden ser víctimas de ataques de ransomware, donde los hackers cifran los datos de la empresa y exigen un rescate para liberarlos. Como menciona el autor Symantec. (2019:16), "Los ataques de ransomware son cada vez más sofisticados, y los ciberdelincuentes están utilizando técnicas avanzadas como el aprendizaje automático y la inteligencia artificial para hacer que sus ataques sean más efectivos". Si la empresa no tiene copias de seguridad de sus datos, puede sufrir una pérdida completa de información y verse obligada a pagar el rescate. Es importante que las empresas, incluyendo las inmobiliarias, tomen medidas para proteger la información sensible que manejan. Esto puede incluir la implementación de software de seguridad, la educación de los empleados en prácticas de seguridad cibernética y la realización de pruebas regulares de vulnerabilidad para identificar las debilidades para así remediarlas.

En el municipio Maneiro, en el estado Nueva Esparta, se está experimentando un auge en el sector inmobiliario, lo que implica que las empresas que operan en este sector manejen información valiosa y sensible, tanto en relación a la infraestructura como a los datos personales de sus clientes. En este sentido, la seguridad de la información de la franquicia inmobiliaria RE/MAX 2Mil C.A., que opera en el municipio Maneiro, depende de la implementación de medidas de seguridad y de la cultura de seguridad de la empresa puede variar; considerando, que el autor de esta investigación labora en la empresa objeto de estudio, se ha podido detectar los riesgos de seguridad informática a los que se podría enfrentar la franquicia inmobiliaria RE/MAX 2Mil C.A. se incluyen: acceso no autorizado a datos confidenciales de los clientes, como información personal, financiera y médica.

A su vez, la suplantación de identidad, en la que un hacker finge ser un cliente legítimo para obtener acceso a la información de la inmobiliaria o incluso para cerrar transacciones fraudulentas. Ransomware, en el que un hacker cifra los datos de la empresa y exige un rescate para restaurarlos. Y por último el phishing, en el que los hackers utilizan técnicas de ingeniería social para obtener acceso a información sensible de la inmobiliaria. Es por eso que la intención de este proyecto consiste en proponer auditoria para los procesos de seguridad de la información de la franquicia inmobiliaria RE/MAX 2Mil del municipio Maneiro, con la intención de garantizar la confidencialidad e integridad de los datos; ya que debe ser una prioridad para la empresa, y mantener la confianza de los clientes.

1.2 Interrogantes

Tomando en cuenta lo expresado en el apartado anterior, es necesario plantear interrogantes que permitan llevar a cabo una investigación ordenada y acorde a la problemática abordada, respecto a la cuestión central de la investigación, las cuales son:

- ¿Cuáles son las áreas de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A. donde presentan vulnerabilidades?
- ¿Cuál es el estado actual de la seguridad informática de la franquicia inmobiliaria RE/MAX 2Mil C.A. en relación con el estándar 27000 y 27001 de la International Organization for Standardization (ISO)?

- ¿Qué estrategias de seguridad informática son las más convenientes para proteger los puntos vulnerables de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A.?

1.3 Objetivo general

- Realizar una auditoría de red para los procesos de seguridad de la información en la franquicia inmobiliaria RE/MAX 2Mil C.A.

1.4 Objetivos específicos

- Evaluar las áreas de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A., donde presenta vulnerabilidades.
- Identificar el estado actual de la seguridad informática de la franquicia inmobiliaria RE/MAX 2Mil C.A. en relación con el estándar 27000 y 27001 de la International Organization for Standardization (ISO).
- Precisar las estrategias de seguridad informática más convenientes para proteger los puntos vulnerables de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A.

1.5 Valor Académico de la Investigación

Resulta provechoso investigar sobre la auditoría de red porque el panorama de amenazas de seguridad informática está en constante evolución, y los métodos utilizados por los atacantes están en constante cambio. Por lo tanto, es importante mantenerse actualizado sobre las mejores prácticas y herramientas de auditoría de red para garantizar la protección efectiva de los sistemas de red de la empresa en un entorno de amenazas en constante evolución.

En el campo de la seguridad de la información, el problema de las brechas de seguridad ha creado un nuevo tópico en el mundo laboral. Se hace hincapié en la necesidad de implementar seguridad avanzada porque las soluciones básicas o aisladas ya no son adecuadas para salvaguardar los recursos de las empresas. Esto incluye capacitación y notificación a los empleados sobre distintas amenazas.

Los conocimientos sobre las materias de: redes de datos, auditoría de sistemas y sistemas operativos se complementan entre sí para ofrecer una visión completa de cómo

se utiliza la tecnología de la información en una empresa. En Redes de datos, e Introducción a las Telecomunicaciones se enseña cómo funcionan las redes informáticas, incluida su topología y los protocolos de comunicación que se emplean. A su vez, la materia Auditoría de sistemas se centra en examinar y evaluar los sistemas de una red, lo que permite recopilar datos útiles sobre las operaciones de la empresa y sugerencias para mejorar la productividad y reducir los riesgos, el conocimiento de Sistemas Operativos también es importante, ya que permite comprender mejor cómo funcionan los sistemas y cómo se relacionan con otros elementos de la red.

Por otra parte, la materia de Seguridad Informática, nos permite saber identificar vulnerabilidades y problemas de seguridad, con el fin de evaluar su cumplimiento con las políticas de seguridad y los requisitos regulatorios; cuando se consideran los hechos mencionados anteriormente en conjunto, es posible comprender mejor los sistemas de información de una organización, por lo tanto, son valiosas para el logro de esta investigación porque es necesario conocer el estado actual de la seguridad empresarial y saber qué medidas son necesarias para certificar el estado ideal de la franquicia inmobiliaria RE/MAX 2Mil.

De igual forma, se consideran los elementos necesarios para proteger los recursos técnicos y de información de las empresas de dicho sector para gestionar frente a amenazas externas intencionales o accidentales con el fin de garantizar la confidencialidad, integridad, disponibilidad, corrección y fiabilidad de la información. El propósito de este estudio es realizar una auditoría de red para los procesos de seguridad de la información para la franquicia inmobiliaria RE/MAX 2Mil. Como resultado, se tendrá conocimiento sobre las amenazas, debilidades y fortalezas de su sistema de tecnología de la información (TI), debido a su enfoque práctico, también puede ser útil para otros académicos y estudiantes interesados en este tema. En consecuencia, puede ayudar a otras empresas, así como también organizaciones del mismo sector a mejorar sus procedimientos para fortalecer la seguridad de sus servicios, logrando satisfacer las necesidades de todos los que dependen de ellas.

PARTE II

DESCRIPCIÓN TEÓRICA

De acuerdo con García, J. (2014, párr. 4) el marco teórico “sirve para acondicionar la información científica que existe sobre lo que se va a investigar, previniendo que el investigador cometa viejos errores en el estudio a desarrollar, dándole guías de cómo hacer el estudio o a dónde dirigirlo”. En este sentido, el presente capítulo se encarga de describir la teoría relacionada con el problema planteado previamente. Se comenzará con algunos antecedentes de la investigación, se explicarán las variables más importantes del estudio y se mencionarán las bases legales relacionadas con el tema en cuestión. Además, se incluirá un glosario de términos.

2.1 Antecedentes de Investigación

En el ámbito de la auditoria de redes y seguridad informática, en los últimos años se han desarrollado muchos tipos de aplicaciones e investigaciones para reducir los riesgos a los que se enfrentan las empresas y apoyar sus actividades. En la preparación de este trabajo de investigación, se consultó la siguiente bibliografía:

Hernández, E. y Nadir, K. (2018), en su trabajo de grado titulado “MANUAL DE AUDITORIA DE LA RED FÍSICA Y LÓGICA EN LA DIRECCIÓN NIC.NI”, el autor llevó a cabo la investigación utilizando un enfoque cualitativo, con el fin de examinar la funcionalidad del sistema, confirmar el cumplimiento de las medidas de seguridad y control necesarias para proteger la integridad de la información del departamento, la evaluación de la misma permitió determinar falencias e identificar oportunidades de mejora o dónde los controles son insuficientes, basándose en los resultados, se emitieron las recomendaciones pertinentes, se empleó la observación y se aplicó una serie de encuestas tanto al personal como a los usuarios del servicio de red.

Adoptando esta perspectiva, según Axelos. (2019) es claro que las actividades de control y verificación de la red informática logran constatar el cumplimiento de las normas internacionales de estandarización en los mecanismos de hardware e instalación de la misma, encontrando hallazgos pertinentes que reflejan la ausencia de buenas prácticas al momento de implementar dichas normas. El hecho de que la red informática sea operativa en la práctica no niega la necesidad de contar con información crítica que

quedó fuera de la implementación de la configuración al momento de basarse en estándares internacionales. En consecuencia, fue posible determinar la situación de la organización y emitir recomendaciones que deberían tenerse en cuenta tanto a corto como a largo plazo.

Ramírez, M. (2011), en su trabajo de grado titulado “AUDITORIA AL CENTRO DE DATOS DE LA UNIVERSIDAD BENITO JUÁREZ”, realizó una investigación exploratoria y descriptiva, aplicando pruebas de penetración a los distintos sistemas de información de dicha institución, con ello se pretende dar a la unidad educativa una medida de la eficacia y eficiencia de los controles establecidos para protegerse y disminuir la posibilidad de que se materialice un riesgo, lo que podría tener un efecto perjudicial en el crecimiento de las operaciones de los servicios ofrecidos a los estudiantes, a la comunidad profesional y provocar pérdidas.

Merece la pena señalar que el autor se refiere a la importancia de realizar una auditoría de seguridad física en un centro de datos y destaca el hecho de que no todas las organizaciones prestan a esta cuestión la atención que merece. Dado que la información que se maneja en estos establecimientos es crítica para el buen funcionamiento de la institución, se menciona que es imprescindible disponer de los controles necesarios para prevenir los peligros, a su vez se subraya que, para gestionar eficazmente la seguridad física de las instalaciones, es preciso disponer de un enfoque adecuado para separar con precisión las funciones de un área o puesto de trabajo determinado.

Mayol, R. (2006), en su trabajo de grado titulado “MODELO PARA LA AUDITORÍA DE LA SEGURIDAD INFORMÁTICA EN LA RED DE DATOS DE LA UNIVERSIDAD DE LOS ANDES”, el autor propone desde un enfoque cuantitativo evaluar el rendimiento de la red mediante la recopilación y el análisis de datos numéricos; a través de un modelo de auditoría completo, equilibrado y técnicamente correcto de la seguridad informática para aquellos servicios de IT que se ofrecen por RedULA para la Universidad de Los Andes, extensible para cualquier entidad de características similares.

Considerado lo anterior, esto es esencial para la investigación, ya que para garantizar la seguridad y protección de los sistemas de una organización se debe enfocar en la estandarización de la auditoría del hardware y medios de almacenamiento de la red, lo

que garantiza que la misma sea correcta, completa y segura; permitiendo a las organizaciones identificar y resolver problemas de vulnerabilidades, lo que garantiza que las amenazas cibernéticas sean reducidas en un ambiente en constante evolución, a su vez, esto puede ser utilizado para la instrucción del personal técnico en los elementos básicos sobre este ámbito.

Según el análisis de los distintos autores, es indispensable que todas las empresas, independientemente de su tamaño, dispongan de métodos y tecnologías para proteger la información de los ciberataques, independientemente del tamaño de la organización, estas medidas de protección se adaptan a las necesidades de cada una de ellas y a su ámbito económico; todos ellos están destinados a garantizar los recursos que posee la misma y garantizando que no se produzcan daños económicos que afecten a la franquicia inmobiliaria RE/MAX 2Mil.

2.2. Bases Teóricas

2.2.1. Auditoria Informática

Según Piattini & Del Peso (2001:4), la auditoria, en su sentido más básico, “es la actividad que conlleva la emisión de una opinión profesional sobre si el objeto analizado presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que han sido prescritas”. He aquí cómo se explica la definición: "el proceso de recopilación, organización y evaluación de datos para valorar si un sistema informático salvaguarda la seguridad e integridad del sistema de información y hace un uso eficiente de los recursos " (Piattini & Del Peso, 2001:28).

Conviene recordar que la auditoría “no es una mera actividad mecánica que consiste en seguir unos pasos para obtener unos resultados que requiere la aplicación de procedimientos, sino que requiere una norma calificada, confiable y razonable para establecer las normativas y para calcular los resultados obtenidos” (Canales Mena, 2006). De esta manera se tratará el tema de la auditoría informática que se preparó para su ejecución en la franquicia Inmobiliaria RE/MAX 2Mil en el estudio de caso que se presenta en este documento.

2.2.2. Auditoria de Redes

Según Tanenbaum (2003), una red informática se describe como “un grupo de ordenadores autónomos conectados entre sí, si dos ordenadores pueden comunicar información, se considera que están interconectados” Del mismo autor se cita lo siguiente: la auditoría de redes se describe como "la revisión exhaustiva, específica y especializada que se realiza en los sistemas de red de una empresa, teniendo en cuenta en la evaluación los tipos de redes, arquitecturas, topología, sus protocolos de comunicación, conexiones, topología, y otros aspectos que inciden."

Tanarro, G. (2010) en su trabajo de investigación indica que “el usuario final de la red apenas va a percibir si su entorno es seguro o no. Su preocupación estará más enfocada a que su conexión tenga la calidad necesaria para poder desarrollar su trabajo sin problema”. Por lo tanto, el auditor informático debe confirmar con frecuencia que los programas realicen exactamente las funciones previstas y no otras. Para ello se utiliza paquetes de software robustos y modulares que, entre otras cosas, rastrean los caminos que siguen los programas. Estas trazas se emplean específicamente para examinar el rendimiento de las validaciones de datos previstas. A su vez, no deben alterar en modo alguno el sistema, las mejores horas y fechas para utilizar la herramienta de auditoría deben decidirse de antemano si da lugar a picos de carga considerables.

2.2.2.1 Auditoria de la Red Física

Tanarro, G. (2010), indica que: “una correcta configuración de los equipos es importante, e influye altamente en el rendimiento de la red. Sin embargo, si queremos obtener buenos resultados, es necesaria una buena infraestructura que de soporte a la electrónica”. El autor indica que se debe cuidar el diseño del cableado que interconecta los distintos equipos que componen la red, tanto entre sí como con los usuarios. De tal manera según Piattini & Del Peso (2001), indica que: “los datos son el primer objetivo de toda seguridad”.

Según Mendoza, A. (2015), menciona en su publicación que la Auditoria de la red física está orientada “en conocer y evaluar los mecanismos de protección del hardware y del cableado”. En este sentido el autor indica que, la misma, “puede considerar la revisión de las conexiones y su apego a normas de cableado estructurado establecidas por

organismos como ANSI o ISO, así como medidas que protegen tanto el cableado como los dispositivos de red”. La seguridad física constituye la utilización de barreras de protección y de control como medidas de prevención y contramedidas contra las amenazas a la información y los recursos confidenciales.

Además de los medios de acceso remoto hacia y desde el centro informático, se utiliza para salvaguardar el hardware y los medios de almacenamiento. La base para empezar a incorporar la seguridad como función primordial en cualquier empresa es evaluar y supervisar continuamente la seguridad física de las instalaciones informáticas y del edificio.

2.2.2.2 Auditoria de la Red Lógica

Según Piattini & Del Peso, (2001), cada vez más se tiende a que un equipo pueda comunicarse con cualquier otro, de manera que sea la red de comunicaciones el común que les une. Leído a la inversa, la red hace que un equipo pueda acceder legítimamente a cualquier otro, incluyendo al tráfico que circule hacia cualquier equipo de la misma. Y todo ello por métodos exclusivamente lógicos, sin necesidad de instalar físicamente ningún dispositivo.

Por lo tanto, Echenique, G. (2002), indica que “se puede concluir que un control de acceso lógico insuficiente aumenta la posibilidad de que la organización pierda información, de que la información sea explotada o de que la información sea utilizada indebidamente”. Los controles de acceso destinados a proteger la integridad de la información son objeto de la seguridad lógica, destinados a evitar el uso indebido de la misma, así como a proteger la información almacenada en un ordenador. De tal manera, Maiwald, E. (2005), indica que “estas salvaguardas disminuyen la posibilidad de encontrarse en circunstancias negativas. Hay que vigilar la red, revisar los errores o situaciones anómalas y disponer de procedimientos para encontrar y aislar los equipos en situación aberrante y apagar los equipos en circunstancias inusuales”.

2.2.3. Pasos para la realización de una Auditoría de Redes

Para llevar a cabo una auditoría, hay que dar varios pasos, el auditor debe evaluar los riesgos generales antes de desarrollar un programa de auditoría que conste de objetivos

de control y procedimientos de auditoría que deben cumplir dichos objetivos. El proceso de auditoría requiere que el auditor recopile pruebas, evalúe los puntos fuertes y débiles de los controles existentes basándose en las pruebas recopiladas y elabore un informe de auditoría que presente estos temas a la dirección de forma objetiva. Además, la dirección de la auditoría debe garantizar la disponibilidad y asignación de recursos suficientes para llevar a cabo el trabajo de la misma, además de las revisiones de seguimiento de las iniciativas de medidas correctoras de la empresa.

El primer paso en la auditoría implica la planificación, que consiste en determinar el tipo de auditoría requerido, documentar los procedimientos necesarios, seleccionar al personal adecuado para llevar a cabo la auditoría y establecer la frecuencia de las mismas (por ejemplo, mensual o anual) .

El segundo paso implica la ejecución de la auditoría de acuerdo con el procedimiento y el plan establecidos. Es recomendable que las auditorías se realicen de manera sistemática y que el director o responsable del área a auditar informe a los empleados con anticipación sobre las fechas en las que se llevarán a cabo las auditorías para que puedan colaborar en el proceso.

El tercer paso es la evaluación de los resultados de la auditoría. Toda auditoría ha de realizarse para obtener una nota final que sirva, aunque solo sea comparativamente, para medir la evolución, tanto de la implementación del sistema, como de la calidad del producto. Y, Por último, la redacción del informe y propuesta de medidas correctoras: una vez valorada la auditoría y antes de la redacción en base a la propuesta de las medidas correctoras, es conveniente la reunión con el director o responsable máximo afectado por la auditoría para que sea el primer informado y pueda incluso colaborar en la propuesta de medidas correctoras, así como en la decisión sobre la urgencia de las mismas.

2.2.4. Sistemas de Información

Según Wangler, B. (2005) define los sistemas de información como “un sistema basado en reglas para la comunicación entre personas en el espacio o en el tiempo”. Es decir, un sistema para enviar, almacenar (y manipular) y recibir (es decir, presentar al receptor) mensajes. Por lo tanto, el componente central, es decir, la base de datos, puede considerarse como una colección de mensajes almacenados. La definición anterior también implica que los sistemas de información no tienen que estar necesariamente informatizados y que, de hecho, cualquier rutina establecida (y basada en reglas) para comunicarse en un entorno organizativo es un sistema de información, y que las personas implicadas participan en dicho sistema.

Sin embargo, los autores Whitten, J., Bentley, L. y Dittman, K. (2004) describen un sistema de información como “un conjunto de personas, datos, procesos y tecnología de la información que interactúan para recoger, procesar, almacenar y proveer la información necesaria para el correcto funcionamiento de la organización”, siendo un sistema de información informatizado, en el que sólo se tiene en cuenta el dispositivo informático de introducción, almacenamiento, manipulación y presentación de la información.

2.2.5. Seguridad Informática

Según Gómez, A. (2006) define la seguridad informática como “cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software”. La seguridad informática sigue siendo un tema crítico en la actualidad, a medida que la tecnología avanza y se vuelve cada vez más omnipresente en la vida cotidiana.

Por su parte, Kissel, R. (2012) la define como “la protección de información y sistemas de información de acceso no autorizado”. La información, que es un activo intangible y muy vulnerable, a su vez, el software, cuya alteración o pérdida puede tener graves repercusiones financieras u operativas para los usuarios y las organizaciones, el hardware, que puede ralentizar las operaciones diarias y resultar dañino, son los tres componentes fundamentales de la seguridad informática. Estos se combinan para formar

un conjunto de elementos cruciales que deben gestionarse de forma adecuada y satisfactoria para garantizar la seguridad de la información y la correcta ejecución de las operaciones de las organizaciones. Además, es fundamental recordar que la seguridad de la información debe considerarse una tarea continua, las amenazas de seguridad informática siguen siendo numerosas y cada vez más sofisticadas, lo que hace que la seguridad informática sea una prioridad cada vez mayor para individuos y organizaciones. Los auditores de redes deben tener un conocimiento profundo de los sistemas informáticos y las posibles amenazas de seguridad, así como de las mejores prácticas y normativas de seguridad.

2.2.5. Análisis de Vulnerabilidad

Según Cordovilla, A. y Sigcho, O. (2020:837), En sistemas de información, la vulnerabilidad se define como "aquel fallo de cualquier tipo que amenaza la seguridad del sistema informático". A su vez, el mismo autor menciona que: "En seguridad informática, la palabra vulnerabilidad se refiere a una debilidad en un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones". Además de ser el resultado de fallos en el diseño del sistema, la vulnerabilidad también puede deberse a la falta de avances tecnológicos o restricciones técnicas del aplicativo.

De tal manera, el portal web de ManageEngine. (s/f). define el análisis de vulnerabilidades como "el proceso de identificar los sistemas en la red que tiene debilidades conocidas o identificadas, como exploits, fallas, brechas de seguridad, puntos de entrada de acceso inseguros y los errores de configuración del sistema". Los autores, Guisao, J. S., & Toro Rendon, J. C. (2014), indican que la detección temprana de vulnerabilidades día cero les permite a las organizaciones tomar acciones de divulgación, informando a entidades y fabricantes, lo cual permitiría contar con tiempos de respuesta rápidos y con acciones que favorezcan a otros posibles afectados; así se evita el daño en los servicios y se mitiga el impacto.

Actualmente, las empresas guardan mucha información electrónicamente. Pero la forma en que estas empresas interactúan entre sí y comparten información en línea puede ser arriesgada y exponer información sensible. Es potencialmente dañina y exhibe

los datos, esta debilidad permite a un atacante violar dichos factores. Dado que los sistemas de información son un componente esencial de las organizaciones, es importante cuidar y proteger la información de cualquier riesgo informático potencial.

2.2.5.1. Exploits

Proveniente de la palabra inglesa Exploit que significa explotar o aprovechar, según Latta, N. (2020) en el foro Avast Academy describe a un exploit como un “programa o secuencia de código diseñados para aprovechar la vulnerabilidad de una aplicación de software y provocar efectos imprevistos”, las vulnerabilidades son áreas débiles en las defensas de un sistema que permiten el acceso a usuarios no autorizados o piratas informáticos.

De otra manera el autor Albors, J. (2022) lo define como “si un modelo de cerradura (sistema o aplicación) tuviera un fallo de diseño que permite a un tercero crear llaves que abran esa cerradura (exploit). Con esta llave, un actor malintencionado podría acceder a un sitio o entorno vulnerable y realizar actos delictivos”. De tal manera se entiende que un exploit es esencialmente una herramienta diseñada para aprovechar una determinada debilidad; si no hay vulnerabilidades, no hay exploits.

2.2.5.1. Puntos de Entrada de Acceso Inseguro

Portolan, M. (2020) menciona que “los puntos de entrada de acceso inseguro son aquellos que permiten acceder a la red a dispositivos o usuarios que no cumplen las normas de seguridad establecidas por la organización”. Los atacantes pueden utilizar estos puntos débiles para poner en peligro la disponibilidad, integridad y confidencialidad de los recursos informáticos de la empresa.

Considerando lo anterior, los autores Piattini & Del Peso (2001) indican que “las aplicaciones ofimáticas gestionan información reservada como agendas de contactos, informes sobre temas confidenciales, estadísticas obtenidas con información extraída de la base de datos corporativa, entre otros. Los accesos no autorizados o las inconsistencias en este tipo de información pueden comprometer el buen funcionamiento de la organización”. Cualquier organización que abra sus servicios informáticos al acceso de la red tendrá que dedicar mucho trabajo a salvaguardar datos y recursos.

Para localizar los puntos de entrada de acceso inseguros y aplicar las medidas correctivas necesarias para salvaguardar la red, es necesario el análisis de vulnerabilidades ya que es una actividad vital. Al inspeccionar las instalaciones, los expertos deben ser conscientes de la contribución potencial de los sistemas de control de acceso, deben saber cómo y cuándo especificarlos para que el acceso pueda controlarse o restringirse eficazmente.

2.2.6. Gobernabilidad IT

Según Hernando, I. (2016), indica que es “es el proceso de validación, definición, distribución, gestión y control de los procesos que garanticen que las IT (Tecnologías de la Información) soporten las estrategias y objetivos organizacionales”. La Gobernabilidad IT establece políticas y estrategias claras para el uso de la tecnología, la asignación de responsabilidades, la definición de funciones y procedimientos relacionados con la Gobernabilidad de IT forman parte de ello. Para garantizar la eficacia y eficiencia de su aplicación, los procesos y políticas de IT también se supervisan, evalúan y mejoran continuamente.

Sin embargo, Saffirio, M. (2006), lo define como “la relación entre el negocio y la gestión informática de una organización”. A su vez, resalta la importación de las materias concernientes a IT en las organizaciones modernas y recomienda que las decisiones estratégicas de IT deban ser tomadas por el director de la misma. La Gobernabilidad de las IT es un tema crucial a tener en cuenta, ya que tiene un gran impacto en la forma en que las empresas gestionan y utilizan las tecnologías de la información. Las organizaciones pueden mejorar su gestión de la misma identificando áreas de mejora y poniendo en práctica las mejores habilidades, gracias al análisis de la Gobernabilidad de IT.

2.2.7. Serie ISO/IEC 27000 y 27001

Estas normas de seguridad fueron publicadas por la Comisión Electrotécnica Internacional (CEI) y la Organización Internacional de Normalización (ISO). Para crear, poner en práctica y mantener al día los requisitos del SGSI, esta ofrece asesoramiento sobre procedimientos de seguridad de la información y se compone principalmente de la

norma ISO/IEC 27001, que define las bases para diseñar un SGSI, haciendo hincapié en la idea de la gestión de la seguridad como un proceso continuo, según EEE. (2019), en su sitio web mencionan que la introducción a la Sección A9 del Anexo A de dicha norma indica: “los usuarios sólo deben tener acceso a la red y a los servicios para los que se les ha autorizado específicamente para usar. El acceso debe ser controlado por un procedimiento de inicio seguro y restringido, de acuerdo con la política de control de acceso”.

La norma ISO/IEC 27001 proporciona un modelo para la creación, documentación e implantación de un SGSI, a su vez, propone un marco de gestión de la seguridad de toda la información de la empresa, incluso si es información perteneciente al propio conocimiento y experiencia de las personas o sea tratada en reuniones. La norma ISO/IEC 27001 protege la confidencialidad, disponibilidad e integridad de los datos de una empresa, mediante un sistema de análisis de los principales riesgos y amenazas que pueden afectar a la información.

Con respecto a la norma ISO/IEC 27002, Ostec (2005) la considera como “una guía completa de implementación de un SGSI, la cual establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización, lo cual incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa”. Entonces, la norma ISO 27001 define cómo gestionar el SGSI, y cuáles son las responsabilidades de los participantes; además, sigue un modelo de planeación y acción continua, siendo sus puntos clave la gestión de riesgos y la mejora continua. Por otro lado, la norma ISO/IEC 27002 ofrece recomendaciones sobre qué medidas tomar para asegurar los sistemas de información de una organización, además de describir los objetivos de control (aspectos a analizar para garantizar la seguridad de la información) y especificar los controles recomendados a implementar.

2.3 Bases legales

2.3.1. Constitución de la República Bolivariana de Venezuela (publicada en Gaceta Oficial Extraordinaria N.º 36.860, de fecha 30 de diciembre de 1.999)

Art. 57.- Toda persona tiene derecho a expresar libremente sus pensamientos, sus ideas u opiniones de viva voz, por escrito o mediante cualquier otra forma de expresión, y de hacer uso para ello de cualquier medio de comunicación y difusión, sin que pueda establecerse censura.

De esta forma, la ley respalda y protege a los investigadores que se ocupen de describir cualquier fenómeno o tema de estudio.

Art. 110.- El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional.

Debido al desarrollo y expansión del país, existe un interés nacional en el avance de la ciencia y la tecnología como herramientas e instrumentos vitales, tanto en el ámbito industrial como en el social. Al establecer la tecnología como una herramienta vital para el desarrollo económico, el uso de la tecnología en las Inmobiliarias permite la expansión de nuevas actividades y empresas, así como la facilitación de las ya existentes, lo cual es reconocido por la Constitución en este artículo.

Art. 156.- Es de la competencia del Poder Público Nacional: (...) 28. El régimen del servicio de correo y de las telecomunicaciones, así como el régimen y la administración del espectro electromagnético (...).

Por lo tanto, en lo que respecta a las telecomunicaciones y el uso seguro de las redes informáticas, el Estado aplicará normas y reglamentos a través de diversos instrumentos legislativos.

2.3.2. Ley Orgánica de Telecomunicaciones (publicada en Gaceta Oficial N.º 39.610, de fecha 7 de febrero de 2011)

Art. 12.- En su condición de usuario de un servicio de telecomunicaciones, toda persona tiene derecho a: 1. Acceder en condiciones de igualdad a todos los servicios de telecomunicaciones y a recibir un servicio eficiente, de calidad e ininterrumpido (...) 2. La privacidad e inviolabilidad de sus telecomunicaciones (...).

En este sentido, cualquier servicio relacionado con las telecomunicaciones, especialmente en materia de telefonía e internet, podrá ser contratado por ciudadanos

físicos y jurídicos, siempre que permita el uso del servicio de forma privada y confidencial.

2.3.3. Ley sobre Protección a la Privacidad de las Comunicaciones (publicada en Gaceta Oficial N.º 34.863, de fecha 16 de diciembre de 1991)

Art. 1. La presente Ley tiene por objeto proteger la privacidad, confidencialidad, inviolabilidad y secreto de las comunicaciones que se produzcan entre dos o más personas.

Mediante el uso de diversas técnicas para castigar a los infractores que intenten extraer información de cualquier dispositivo de comunicación o almacenamiento sin permiso, pretende garantizar la confidencialidad de los datos transmitidos a través de las telecomunicaciones.

2.3.4. Ley sobre el Derecho de Autor (publicada en Gaceta Oficial Extraordinaria N.º 4.638, de fecha 1 de octubre de 1993)

Art. 1. Las disposiciones de esta Ley protegen los derechos de los autores sobre todas las obras del ingenio de carácter creador, ya sea de índole literaria, científica o artística, cualquiera sea su género, forma de expresión, mérito o destino (...).

Art. 2. Se consideran comprendidas entre las obras del ingenio a que se refiere el artículo anterior, especialmente las siguientes: los libros, folletos y otros escritos literarios, artísticos y científicos, incluidos los programas de computación, así como su documentación técnica y manuales de uso (...).

La ley salvaguarda los derechos de propiedad intelectual asociados a todos los trabajos de investigación y obras originales producidas por seres humanos, ya sea individual o colectivamente, y complementa ambos artículos.

2.3.5. Ley Especial Contra los Delitos Informáticos (publicada en Gaceta Oficial N.º 37.313, de fecha 30 de octubre de 2001)

Art. 1. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

Como se indica en el citado artículo, esta ley aborda especialmente el problema de los ataques informáticos y los esfuerzos de sabotaje empresarial a nivel de los sistemas

informáticos, definiendo directrices y sanciones para quien infrinja alguna de las disposiciones contenidas en la misma.

2.4 Definición de Términos

Ataque:

“Aquella acción que puede llevar a cabo una persona contra otra”. (Flores, U. 2009)

Amenaza:

“Situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan”. (Tarazona, 2007).

Ataque informático:

“Consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema”. (Mieres, 2009).

Circuito Cerrado de Televisión (CCTV):

Es un sistema de seguridad que graba y supervisa el comportamiento en una zona específica mediante cámaras de vídeo. Los profesionales de la seguridad pueden ver las fotos en tiempo real mientras inspeccionan los registros gracias a la conexión de las cámaras a un sistema centralizado de grabación y supervisión. (Definición propia).

Dirección MAC:

“Es un identificador único hexadecimal de 48 bits que se utiliza para identificar de forma inequívoca a un determinado dispositivo de red”. (Rubén, 2018).

Dirección IP:

“Es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de vídeo o la conexión a un sitio web. Una dirección IP identifica una red o dispositivo en Internet”. (Patrizio, 2019).

Ethernet:

“Es la tecnología tradicional para conectar dispositivos en una red de área local (LAN) o una red de área amplia (WAN) por cable, lo que les permite comunicarse entre sí a través de un protocolo”. (Burke, J., Irei, A., & Chai, W. ,2021).

Firewall:

“Es un sistema o un grupo de sistemas que implementan una política de control de acceso entre dos o más redes”. (Martínez, K. 2009).

LAN:

“La local área network generalmente llamadas LAN, son redes de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión”. (Tanenbaum, A. 2012).

Pentesting:

“Es un ataque simulado y autorizado contra un sistema informático con el objetivo de evaluar la seguridad del sistema. Durante la prueba, se identifican las vulnerabilidades presentes en el sistema y se explotan tal como haría un atacante con fines maliciosos”. (Guillén, J. 2017).

Protocolos:

“Son reglas o estándares que definen la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores, y pueden ser implementados por el hardware y el software”. (Turolto, 2015).

Red inalámbrica:

“Utilizan el aire o el espacio para poder transmitir los datos sin uso de cables, mediante ondas electromagnéticas como wifi o bluetooth”. (Proaño, 2015).

Red alámbrica:

“Se describen como una disposición que involucra un cableado para establecer enlaces a Internet, con computadores y con otros dispositivos en la red. Los datos se transfieren de un dispositivo a otro mediante cables Ethernet. (Corvo, H. 2019).

Servidor:

“Son equipos informáticos que brindan un servicio en la red, dando información a otros servidores y a los usuarios”. (Marchionni, 2011).

Servidor local:

“Es un servidor que está ubicado físicamente en la misma ubicación que las personas o empresas que le dan uso”. (Borges, 2020).

Vulnerabilidad:

“Debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se considera una característica propia de los sistemas de información o de la infraestructura que los contiene”. (Tarazona, 2007).

PARTE III

DESCRIPCIÓN METODOLÓGICA

Tamayo y Tamayo (2003:37), define al marco metodológico como “un proceso que, mediante el método científico, procura obtener información relevante para entender, verificar, corregir o aplicar el conocimiento”, dicho trabajo de investigación pertenece a la línea de investigación número 5, llamada “MÉTODOS Y ESTANDARIZACIÓN DE SISTEMAS” y conformado por el área temática “AUDITORIA”, además que, dicho conocimiento se adquiere para relacionarlo con las hipótesis presentadas ante los problemas planteados. De este modo, en esta sección se describirá la naturaleza de la investigación, incluidos el tipo, el diseño, la población y la muestra del estudio, así como las técnicas de recogida y análisis de datos que se utilizaron en esta investigación.

3.1. Naturaleza de la Investigación

De acuerdo con Tamayo (2007), la investigación cuantitativa, consiste en “el contraste de teorías ya existentes a partir de una serie de hipótesis surgidas de la misma, siendo necesario obtener una muestra, ya sea en forma aleatoria o discriminada, pero representativa de una población o fenómeno objeto de estudio”. Se realizó una auditoría exhaustiva de la red con el fin de analizar objetivamente la situación de la seguridad de la franquicia inmobiliaria RE/MAX 2Mil, al centrar el análisis en un área específica de la lógica y abordar los aspectos pertinentes de las redes de datos; es posible sugerir medidas preventivas y correctivas para mitigar los riesgos que se han identificado. Para alcanzar este objetivo, se implementó un enfoque cuantitativo que permita utilizar numerosos recursos de este tipo para desarrollar una perspectiva teórica sólida.

3.1.1. Tipo de investigación

Según Sabino (1986:51), en la investigación de tipo descriptiva “trabaja sobre realidades de hechos, y su característica fundamental es la de presentar una interpretación correcta”. El objetivo principal de la investigación descriptiva es descubrir algunas características esenciales de conjuntos homogéneos de fenómenos mediante el empleo de criterios sistemáticos que permitan demostrar su estructura o comportamiento. Así, es posible obtener las notas que describen la realidad estudiada. A su vez, según

UPEL (1998:7) define el proyecto factible como un estudio “que consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para solucionar problemas, requerimientos o necesidades de organizaciones o grupos sociales”. De tal manera utilizando herramientas de análisis y evaluación de seguridad informática, este trabajo de investigación descriptiva se centró en la representación y comprensión de los factores relacionados con los niveles de seguridad y control de acceso de la franquicia inmobiliaria RE/MAX 2Mil, a su vez, se proporcionó una descripción detallada de los aspectos relacionados con la seguridad de la arquitectura de red de la compañía, siendo el objetivo principal de esta investigación.

3.1.2. Diseño de la investigación

Según Tamayo y Tamayo (2003:110), menciona que una investigación de campo “es aquella que permite recoger los datos directamente de la realidad, por lo cual se denomina primarios, su valor radica en que permiten cerciorarse de las verdaderas condiciones en que se ha obtenido la información”. A su vez, Bavaresco (2001:26) afirma que: “los estudios de campo o también conocido como “in situ”, de esta manera permite al investigador conocer más a fondo el tema y manejar los datos con más confianza. Finalmente, esta investigación está vinculada con la modalidad de los estudios de campo, ya que la información y los datos necesarios para la realización de la misma fueron obtenidas directamente de la franquicia inmobiliaria RE/MAX 2Mil en la cual se efectúa el estudio.

3.1.3. Población y Muestra

Considerando que Arias (1999:98) señala que, la población “es el conjunto de elementos con características comunes que son objetos de análisis y para los cuales serán válidas las conclusiones de la investigación”. A su vez, para Balestrini (1997:138), la muestra “es obtenida con el fin de investigar, a partir del conocimiento de sus características particulares, las propiedades de una población”. De esta manera la población de la presente investigación es la oficina inmobiliaria franquiciada RE/MAX 2Mil compuesta por las siete personas del departamento de administración y nueve agentes asociados a la marca, por su parte la muestra está representada por la totalidad de la población es decir el 100%.

3.1.4. Técnicas de Recolección de Datos

Es crucial elegir las técnicas de recopilación de datos adecuadas para el objetivo específico de la auditoría de la red y asegurarse de que se utilizan de forma rigurosa y objetiva para obtener resultados precisos y fiables. Según Tamayo (1999:126), las técnicas de recolección de datos, son definidas como “la expresión operativa del diseño de investigación y que especifica concretamente como se hizo la misma”. Se empleará técnicas como la Observación Directa.

Los autores Hernández, Fernández y Baptista (2006: 316), definen la observación directa como: “el registro sistemático, válido y confiable de comportamientos o conducta manifiesta”. El investigador registra lo que sucede sin influir en los eventos o alterarlos de alguna manera. Por lo tanto, consiste en observar directamente los sistemas y dispositivos de la red y sus interacciones para identificar posibles problemas, vulnerabilidades o violaciones de políticas de seguridad.

Por otro lado, también se utilizó la entrevista, el cual Sabino (1992:116) autor que comenta que la entrevista, desde el punto de vista del método es “una forma específica de interacción social que tiene por objeto recolectar datos para una investigación”. Estas pueden llevarse a cabo con usuarios y administradores de la red para conocer mejor cómo se utilizan los sistemas y los recursos de la red, detectar posibles problemas; para así obtener opiniones de los usuarios sobre el rendimiento y la seguridad de la misma.

Según Hernández, Fernández y Baptista (2006:310) definen la encuesta como “el instrumento más utilizado para recolectar datos, consiste en un conjunto de preguntas respecto a una o más variables a medir”. No obstante, se logra obtener información cuantitativa sobre cómo se están utilizando los sistemas y recursos de la red, identificar las áreas problemáticas sobre la seguridad y el rendimiento de la red.

3.1.4. Técnicas de Análisis de Datos

Según Arias (2004:99), "en este punto se describen las distintas operaciones a las que serán sometidos los datos que se obtengan". Para obtener resultados precisos y fiables, es fundamental elegir las metodologías de análisis de datos adecuadas para el objetivo concreto del presente trabajo de investigación y aplicarlas de forma exhaustiva y objetiva.

En virtud de ello, el análisis estadístico se utiliza para procesar y analizar datos cuantitativos, para identificar patrones y tendencias en los datos; para determinar problemas de rendimiento, establecer el uso y la carga de la red, y para detectar posibles amenazas, según Chávez (2004) la tabulación es “el proceso del análisis estadístico de los datos”. Para determinar el número de casos, se tiene en cuenta el contenido de las respuestas obtenidas. Según Tamayo y Tamayo (2007) la tabulación “permite organizar los datos para aplicar las estadísticas correspondientes, a fin de procesar la información”.

Según Cohen & Swerdik, (2001), la validez de contenido consiste “en qué tan adecuado es el muestreo que hace una prueba del universo de posibles conductas, de acuerdo con lo que se pretende medir”. Para ello se examinan los datos recopilados del ámbito de la auditoría de redes con el fin de confirmar si los datos suministrados son pertinentes y exhaustivos para el estudio.

Según Hernández, Fernández y Baptista (2006), la distribución de frecuencias “facilita la exposición ordenada de la totalidad de las observaciones de las que se dispone, de una o más variables estadísticas mediante el recuento de las apariciones de cada aspecto evaluado expresado en números absolutos y en porcentaje, tomando como referencia a la totalidad de la población”. En esta investigación, se logra determinar el comportamiento de los usuarios, los patrones de tráfico de la red y las tendencias de consumo de la red. Se utiliza para determinar la frecuencia con la que se produce un evento específico.

PARTE IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

El análisis e interpretación de los resultados según Hurtado (2010, p. 181), “son las técnicas de análisis que se ocupan de relacionar, interpretar y buscar significado a la información expresada en códigos verbales e icónicos”. Al respecto, Talaya (2008, p. 302) afirma que el análisis de los datos, teniendo en cuenta las características de los objetos específico, las variables estudiadas y los instrumentos aplicados, se organizan por ítems, tabulador, el número de respuesta frecuencia, calculando el porcentaje de respuestas dada por la muestra seleccionada y finalmente se grafica en esta etapa de la investigación cualitativa y cuantitativa de los porcentajes de respuestas de los distintos ítems, orientado siempre al análisis en el contexto de los objetivos de la investigación.

En la siguiente sección expondremos las generalidades de la institución para la comprensión de los resultados y los hallazgos como parte del estudio realizado a la infraestructura física y lógica de la red de computadoras, basada en estándar ISO 27000, con los dominios “Políticas de Seguridad”, “Administración de Recursos”, “Seguridad de los recursos humanos”, “Administración de operaciones y comunicación” y “Control de Acceso” y basada en la ISO 27001, con los dominios de: “Política de Seguridad”, “Organización de la Seguridad de la Información”, “Gestión de Activos”, “Seguridad de los Recursos Humanos”, “Seguridad física y del ambiente”, “Gestión de las comunicaciones y operaciones” y “Control de Acceso”. Para efectos de comprensión el siguiente párrafo contendrá en su totalidad el informe ejecutivo de Auditoría.

4.1 Evaluación de las áreas de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A., donde presenta vulnerabilidades.

RE/MAX, la empresa Líder mundial en Bienes Raíces fue fundada en Denver, Colorado, en 1973 por Dave y Gail Liniger, dos exitosos corredores inmobiliarios quienes diseñaron un modelo de negocio innovador para reclutar y retener a los mejores vendedores del mercado, ofreciéndole servicios y apoyo gerencial para que maximicen sus captaciones y sus transacciones inmobiliarias.

RE/MAX se ha expandido a los 5 Continentes, sumando más de 140.000 Agentes Asociados y más de 9.000 Oficinas, ubicadas en 110 Países. En Venezuela existen más de 1.700 Agentes Asociados y más de 80 oficinas ubicadas en las ciudades principales con oportunidades de crecimiento a lo largo y ancho del país. La franquicia inmobiliaria REMAX 2Mil que se compone de dos departamentos, el administrativo y los franquiciados, ubicada en la isla de Margarita es la seleccionada para llevar a cabo la auditoría efectiva de la red de este trabajo de investigación.

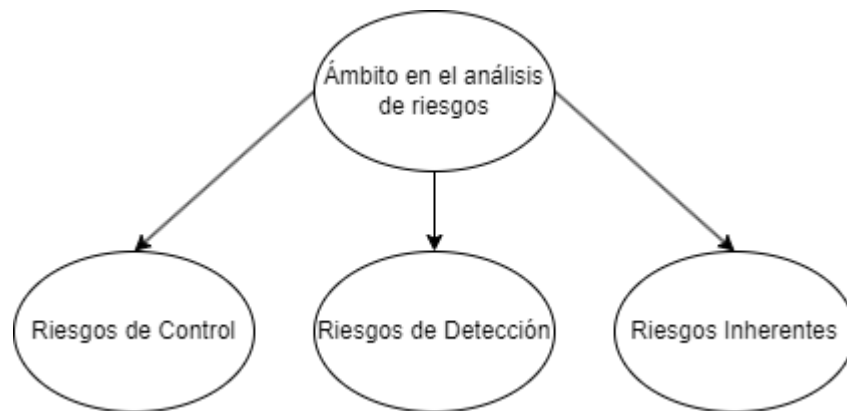
Los departamentos de la empresa trabajan juntos para garantizar que las operaciones diarias funcionen sin problemas. El departamento administrativo se encarga de la gestión de la empresa, la contabilidad, la administración de recursos humanos y el cumplimiento de la normativa legal. Por otro lado, los franquiciados son los encargados de llevar a cabo las transacciones inmobiliarias con los clientes y realizar la gestión de las propiedades.

De tal manera, el riesgo se define como la probabilidad de que una o varias amenazas se materialicen y provoquen un suceso catastrófico. Las vulnerabilidades o amenazas por sí solas no suponen una amenaza inmediata. Sin embargo, cuando se combinan, suponen un riesgo, o la posibilidad de que se produzca una catástrofe. El término "riesgo" se refiere a la "probabilidad de sufrir daños o experimentar errores" en determinadas circunstancias.

En el ámbito de la auditoría de la seguridad de la información, como se puede observar en el gráfico 1, con título "Clasificación de riesgos", este se clasifica en tres categorías, riesgos de detección: es el riesgo de que un auditor no detecte una representación errónea que exista en una aseveración y que pudiera ser de importancia relativa, ya sea en lo individual o cuando se acumula con otras representaciones erróneas (Federación Internacional de Contabilidad, 2007).

Los Riesgos de Control, que serían una representación errónea que pudiera ocurrir en una aseveración y que pudiera ser de importancia relativa, ya sea en lo individual o cuando se acumula con representaciones erróneas en otros saldos o clases, no se prevenga o detecte y corrija oportunamente por el control interno de la entidad (Federación Internacional de Contabilidad, 2007). Y por último los riesgos inherentes: El riesgo que se somete una organización en ausencia de acciones de la administración para alterar o reducir su probabilidad de ocurrencia e impacto (Cartaya, 2009).

Gráfico 1. Clasificación de riesgos

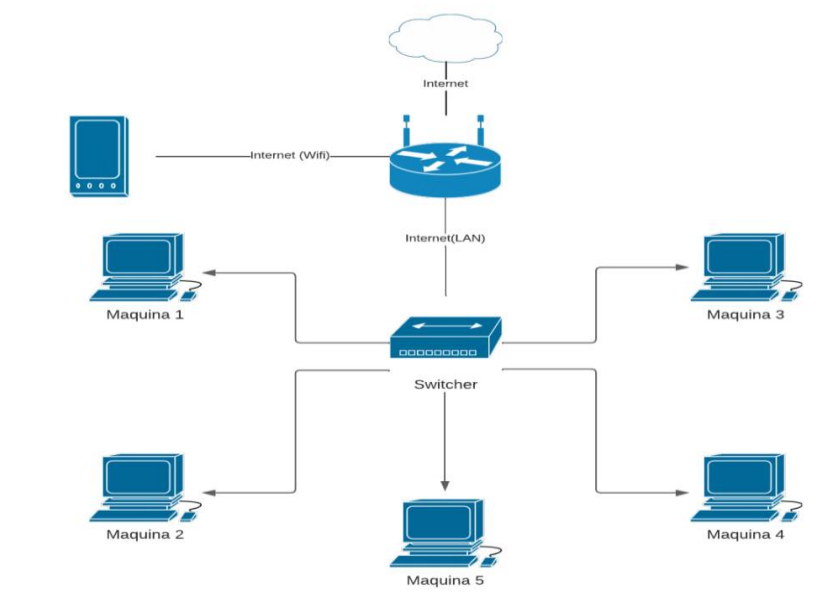


Fuente: Elaboración propia (2023).

En la oficina de la franquicia inmobiliaria RE/MAX 2Mil La topología de red que está llevada a cabo es de estrella, como se puede observar en el gráfico 2, con título “Topología de red de RE/MAX 2Mil” esta suele emplearse por su sencillez y facilidad de administración. En esta arquitectura, se encuentran 5 ordenadores fijos que están conectados a un dispositivo central, que sirve de punto de distribución de la información entre todos los ordenadores conectados.

La topología en estrella es muy útil en una empresa con pocos ordenadores conectados a la red de área local (LAN), ya que permite una conexión y comunicación sencillas entre ellos. Además, en este escenario, todos los dispositivos tanto laptops como smartphones pueden unirse a una red Wi-Fi con seguridad solo para agentes asociados, lo que simplifica la conexión a Internet y abre la puerta al uso compartido de recursos. Sin embargo, en una empresa donde no se lleven a cabo controles de seguridad y de acceso a la red puede ser obtenido por quienes tienen malas intenciones.

Gráfico 2. Topología de red de RE/MAX 2Mil



Fuente: Elaboración propia (2023).

4.2 Identificación del estado actual de la seguridad informática de la franquicia inmobiliaria RE/MAX 2Mil C.A. en relación con el estándar 27000 y 27001 de la International Organization for Standardization (ISO).

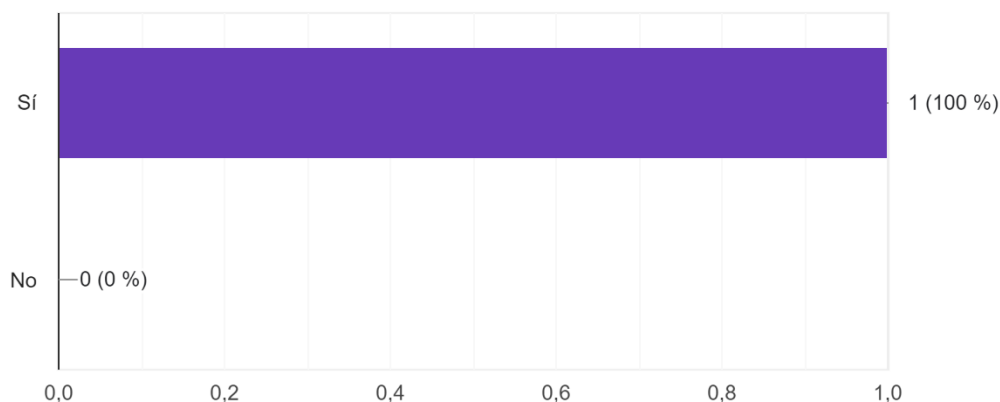
Con motivo de identificar el estado actual de la seguridad informática de la franquicia inmobiliaria RE/MAX 2Mil C.A., se realizó dos encuestas de preguntas cerradas, la primera dirigida al bróker de la compañía y otra encuesta dirigida a los agentes asociados a la franquicia, luego de explicar cómo debían responder la encuesta, procedieron a responder las preguntas a través de la plataforma Google Forms, lugar donde se encuentran las preguntas.

Entrevista estructurada realizada al bróker de la compañía:

1. ¿La inmobiliaria proporciona una red informática para la gestión de las operaciones en su franquicia?

En la encuesta realizada al broker de la inmobiliaria, respondió afirmativamente a esta pregunta, indicando que la empresa dispone de una red informática para la gestión de las operaciones. Desempeñando un papel clave en la optimización de los procesos internos de la empresa. Permitiendo a los agentes acceder a una base de datos centralizada que contenga información relevante sobre propiedades disponibles, clientes potenciales y otros datos importantes para el negocio inmobiliario. Agilizando el proceso de búsqueda y asignación de propiedades a los clientes, así como mejorar la comunicación interna y la colaboración entre los miembros del equipo.

Gráfico 3. La inmobiliaria proporciona una red informática



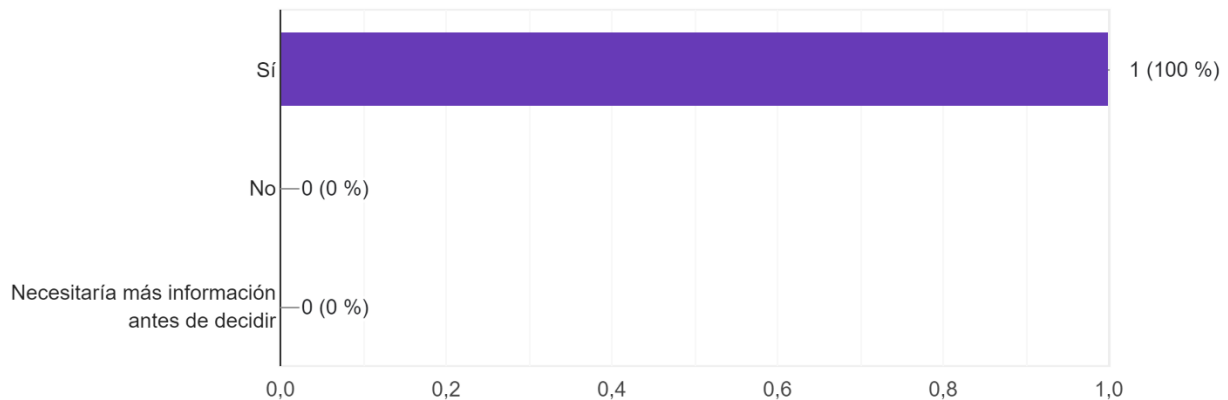
Fuente: Elaboración propia (2023).

2. ¿Estaría dispuesto a colaborar y proporcionar acceso a la infraestructura de red de su franquicia para llevar a cabo una auditoría?

El broker respondió afirmativamente a esta pregunta, indicando que estaría dispuesto a colaborar y facilitar el acceso a la infraestructura de red para realizar la auditoría, esto demuestra una actitud abierta y transparente por parte de la empresa inmobiliaria. Ya que implica la voluntad de someterse a una evaluación exhaustiva de los sistemas y procesos internos. La voluntad de colaborar y permitir el acceso a la infraestructura de la red

también demuestra un compromiso con la transparencia y la calidad de los servicios ofrecidos. Al permitir una auditoría, la inmobiliaria muestra su voluntad de cumplir las normas de calidad, proteger la información de los clientes y garantizar la eficiencia operativa.

Gráfico 4. Dispuesto a colaborar y proporcionar acceso a la infraestructura



Fuente: Elaboración propia (2023).

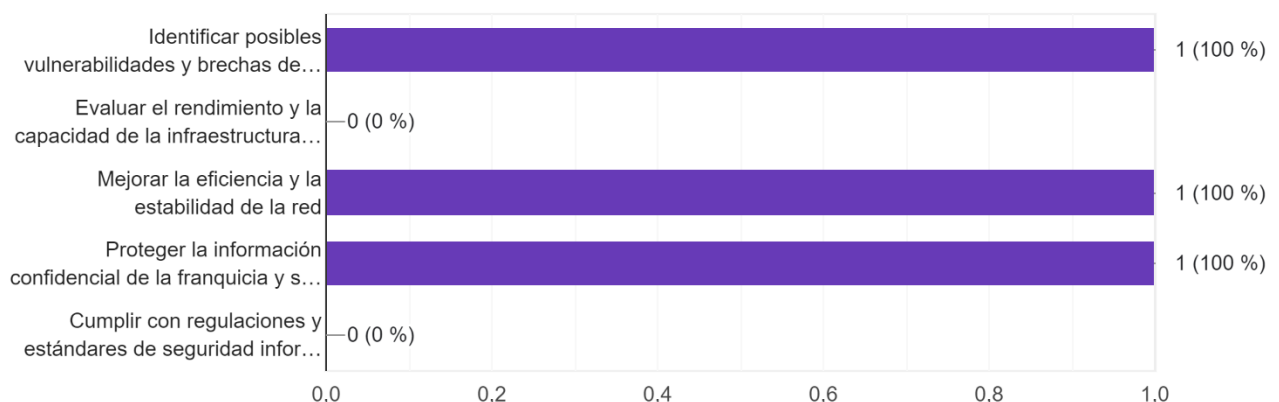
3. ¿Cuál considera que es la importancia de realizar una auditoría de red en su franquicia? (Seleccione todas las opciones que apliquen)

El broker en la encuesta seleccionó tres opciones como respuesta: identificar posibles vulnerabilidades y brechas de seguridad en la red, mejorar la eficiencia y estabilidad de la red, y proteger la información confidencial de la franquicia y sus clientes. Estas opciones seleccionadas reflejan una clara comprensión de los beneficios y la importancia de realizar una auditoría de red en la franquicia inmobiliaria. Identificar posibles vulnerabilidades y brechas de seguridad en la red es una preocupación crítica en el entorno actual de ciberamenazas, esto es especialmente importante en un sector como el inmobiliario, donde la confidencialidad y la protección de datos son primordiales.

Mejorar la eficiencia y la estabilidad de la red es otra de las principales ventajas de realizar una auditoría. Al evaluar la infraestructura de red existente, se pueden identificar áreas de mejora y optimización. Esto puede implicar la actualización de equipos, la optimización de la configuración de la red o la implementación de soluciones más

eficientes. Una red estable y eficiente garantiza un flujo de trabajo fluido y una comunicación eficaz dentro de la franquicia. Y, por último, proteger la información confidencial de la franquicia y sus clientes es un aspecto crítico del negocio inmobiliario. Los datos sobre propiedades, transacciones y clientes son valiosos y deben protegerse adecuadamente.

Gráfico 5. Importancia de realizar la auditoria en la franquicia



Fuente: Elaboración propia (2023).

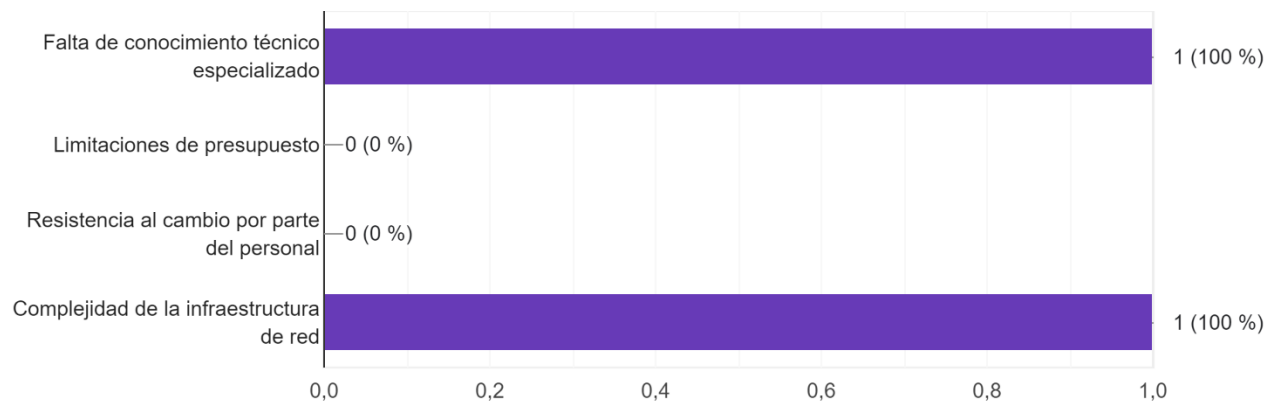
4. ¿Cuáles cree que podrían ser los principales desafíos u obstáculos al realizar una auditoría de red en su franquicia? (Seleccione todas las opciones que apliquen)

La pregunta se refiere a los principales retos u obstáculos a la hora de realizar una auditoría de red en su franquicia. El broker seleccionó dos opciones como respuesta: la falta de conocimientos técnicos especializados y la complejidad de la infraestructura de red. Estas opciones seleccionadas identifican dos retos comunes que pueden surgir al realizar una auditoría de red en una franquicia inmobiliaria.

La falta de conocimientos técnicos especializados puede ser un obstáculo importante, especialmente si no se dispone de personal interno o externo con experiencia en auditoría de redes. Si la franquicia carece de personal formado en este ámbito, puede resultar difícil llevar a cabo una auditoría de forma eficaz y exhaustiva. La complejidad de la infraestructura de red también puede plantear problemas durante una auditoría ya que

puede aumentar el tiempo y los recursos necesarios para realizar una auditoría exhaustiva.

Gráfico 6. Principales desafíos al realizar la auditoria en la franquicia



Fuente: Elaboración propia (2023).

A continuación, la segunda Encuesta estructurada realizada a los agentes de la compañía:

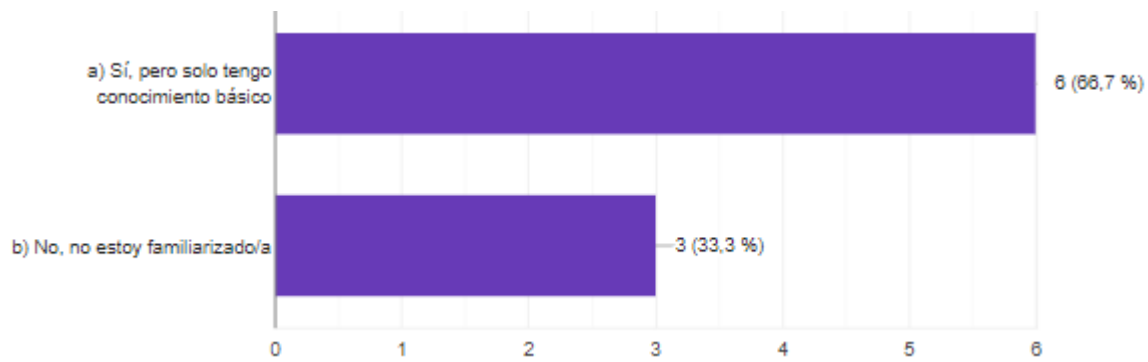
1. ¿Está familiarizado/a con las políticas y procedimientos de seguridad de la red implementados por la compañía?

En la encuesta realizada a los agentes franquiciados de la inmobiliaria, se les preguntó si conocían las políticas y procedimientos de seguridad de la red implementados por la empresa. De las respuestas recibidas, 6 personas respondieron afirmativamente ("Sí") y 3 respondieron negativamente ("No"). La respuesta positiva de 6 agentes indica que conocen y están familiarizados dichas políticas, se trata de un aspecto alentador, ya que demuestra que un grupo significativo de agentes comprende y sigue las medidas de seguridad adecuadas.

Estar familiarizado con estas políticas y procedimientos es fundamental para garantizar un entorno seguro y proteger la información confidencial tanto de la empresa como de sus clientes. Sin embargo, también es importante señalar que 3 agentes indicaron que no estaban familiarizados con las políticas y procedimientos de seguridad de la red. Esta respuesta plantea un punto de atención, ya que la falta de conocimientos puede

aumentar el riesgo de violaciones de la seguridad y poner en peligro la integridad de los datos tanto de los usuarios como de la empresa.

Gráfico 7. Familiarización con las políticas y procedimientos de seguridad



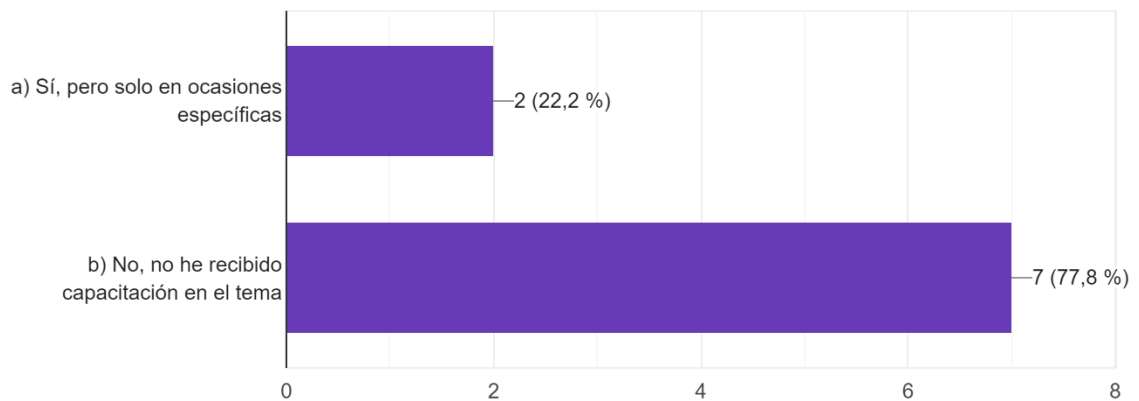
Fuente: Elaboración propia (2023).

1. ¿Ha recibido capacitación sobre buenas prácticas de seguridad informática y protección de la red en el entorno laboral?

Según las respuestas obtenidas, 2 agentes respondieron afirmativamente ("Sí") y 7 personas respondieron negativamente ("No"). La respuesta positiva indica que han recibido capacitación sobre buenas prácticas de seguridad informática y protección de la red en el entorno laboral. Esta capacitación puede ser de gran valor, ya que les brinda los conocimientos y las habilidades necesarias para mantener un entorno seguro y proteger la red contra amenazas potenciales.

Estos agentes pueden aplicar estas buenas prácticas en su trabajo diario, lo que contribuye a la protección de la información confidencial y a la prevención de violaciones de seguridad. Sin embargo, es preocupante que la mayoría de los agentes, es decir, 7 personas, hayan indicado que no han recibido capacitación. Dicho aspecto puede ser una falta grave que podría aumentar el riesgo de errores y violaciones de seguridad a futuro, lo que dañaría la integridad de los datos y la reputación de la compañía.

Gráfico 8. Capacitación sobre prácticas de seguridad informática en el entorno laboral

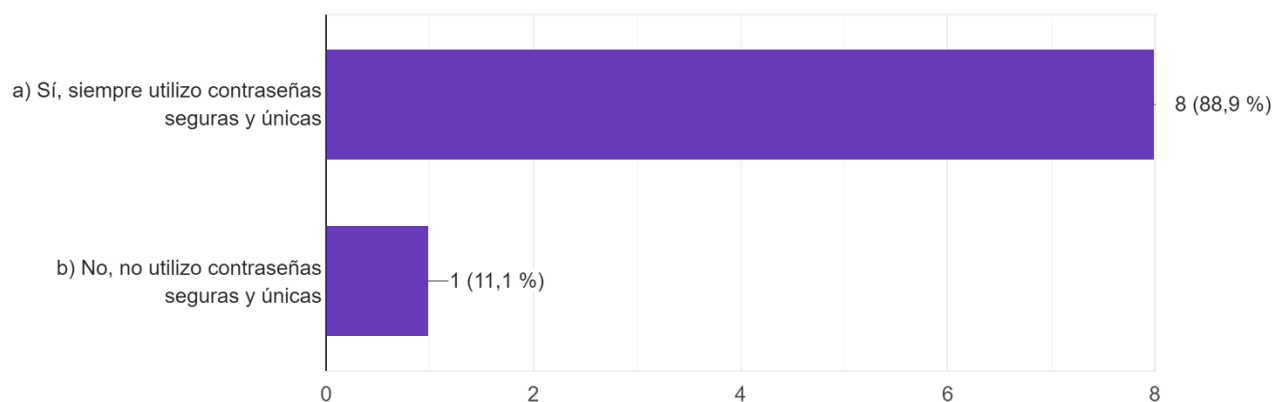


Fuente: Elaboración propia (2023).

2. ¿Cuenta con contraseñas seguras y únicas para acceder a los sistemas y recursos de la red de la compañía?

De las respuestas obtenidas, 8 personas respondieron afirmativamente ("Sí") y 1 persona no respondió. La respuesta positiva indica que están conscientes de la importancia de utilizar contraseñas seguras y únicas para acceder a los sistemas y recursos de la red de la compañía. El uso de contraseñas seguras ayuda a proteger los datos y la información confidencial de la franquicia y sus clientes contra accesos no autorizados. Esto es crucial en un entorno donde la seguridad de la red y la protección de la información son de vital importancia. Sin embargo, es necesario abordar la falta de respuesta de 1 persona, ya que no se puede determinar si cuenta o no con contraseñas seguras y únicas. Es importante recordar a todos los agentes la importancia de utilizar contraseñas robustas, que combinen letras, números y caracteres especiales, así como evitar el uso de información personal fácilmente deducible.

Gráfico 9. Contraseñas seguras para acceder a los recursos de la compañía



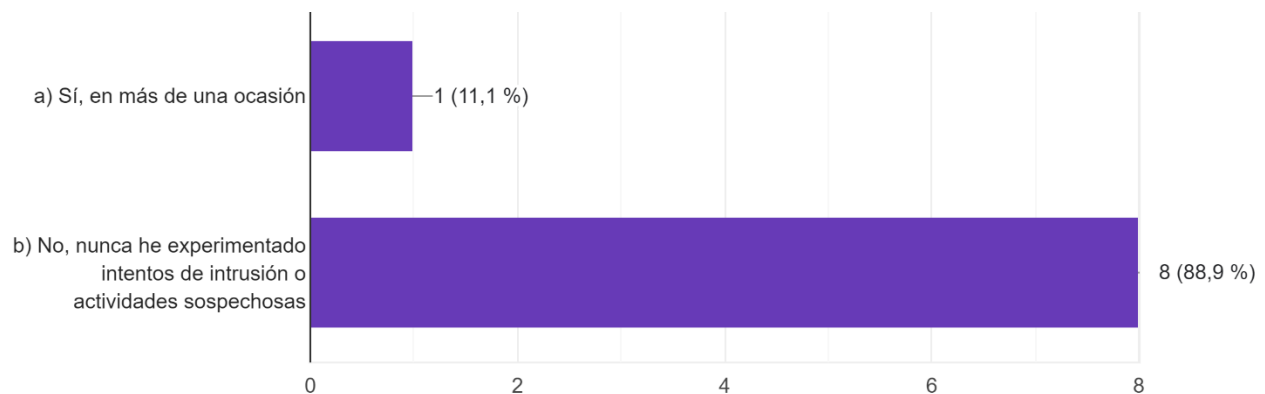
Fuente: Elaboración propia (2023).

3. ¿Ha experimentado alguna vez intentos de intrusión o actividades sospechosas en la red de la compañía?

En la encuesta realizada a los agentes franquiciados de la compañía inmobiliaria, se les preguntó si habían experimentado alguna vez intentos de intrusión o actividades sospechosas en la red de la compañía. De las respuestas obtenidas, 1 agente respondió afirmativamente ("Sí") y 8 agentes respondieron negativamente ("No").

La respuesta positiva de 1 persona indica que ha experimentado intentos de intrusión o actividades sospechosas en la red de la compañía. Esto es un motivo de preocupación, ya que puede indicar posibles vulnerabilidades en la seguridad de la red. Es relevante destacar que 8 personas respondieron negativamente a la pregunta, esto puede deberse a la falta de experiencia en reconocer intentos de intrusión o la falta de conocimiento sobre cómo identificar actividades sospechosas. Sin embargo, esto también puede indicar una falta de conciencia o una falta de comunicación efectiva sobre la importancia de informar sobre intentos de intrusión maliciosas en la compañía.

Gráfico 10. Experimentados intentos de intrusión o actividades sospechosas en la red de la compañía



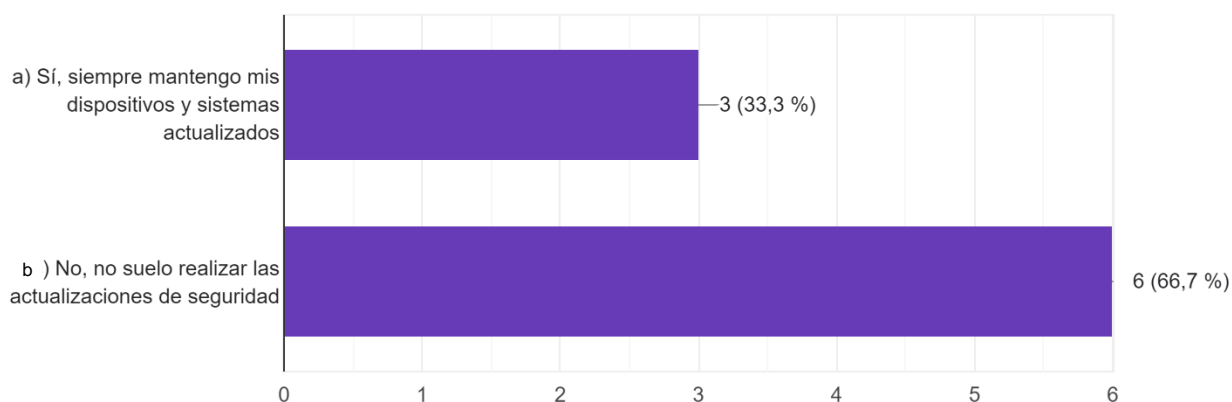
Fuente: Elaboración propia (2023).

4. ¿Cumple regularmente con las actualizaciones de seguridad y parches proporcionados para los dispositivos y sistemas que utiliza en su trabajo?

De las respuestas obtenidas, 3 personas respondieron afirmativamente ("Sí") y 6 personas respondieron negativamente ("No"). La respuesta positiva indica que están conscientes de la importancia de mantener actualizados los dispositivos y sistemas utilizados en su trabajo. Las actualizaciones de seguridad y parches proporcionados por los fabricantes y proveedores suelen contener correcciones de vulnerabilidades y mejoras de seguridad que ayudan a proteger contra amenazas y riesgos cibernéticos.

Al cumplir con estas actualizaciones regularmente, estos agentes demuestran un compromiso con la seguridad de la red y la protección de la información confidencial. Sin embargo, es preocupante que la mayoría de los agentes, es decir, 6 personas, hayan indicado que no cumplen regularmente con las actualizaciones de seguridad y parches. La falta de actualizaciones puede dejar los dispositivos y sistemas vulnerables a ataques y brechas de seguridad, lo que podría comprometer la integridad de la red y la confidencialidad de la información.

Gráfico 11. Cumplen regularmente las actualizaciones y parches de seguridad



Fuente: Elaboración propia (2023).

A continuación, se mencionarán las vulnerabilidades que se identificaron a través de las herramientas de recopilación de datos, a su vez, las recomendaciones se basan en los hallazgos identificados durante la auditoría y en la comparación con los requisitos de la norma ISO 27001. Se recomienda que la franquicia inmobiliaria RE/MAX 2Mil implemente el plan de acción para abordar los hallazgos y mejorar la seguridad de su red de acuerdo con las mejores prácticas de seguridad de la información.

En la oficina de RE/MAX 2Mil carece de una segmentación adecuada, lo que significa que no se han establecido particiones o zonas separadas en la red para diferentes tipos de usuarios, sistemas o servicios. Esto aumenta el riesgo de propagación de amenazas en caso de incidente de seguridad informática. En comparación con ISO 27001, en su control A.10.1.1 (Gestión de la seguridad de la red), establece la necesidad de segmentar las redes y separar las zonas de mayor riesgo. Este control se centra en limitar la exposición de los activos de información y minimizar el impacto potencial de un incidente de seguridad mediante una adecuada segmentación de la red.

Se ha identificado que no tiene un enfoque estructurado para controlar el acceso a la red y a los recursos. Esto implica que no existen políticas y procedimientos claros para gestionar y controlar los derechos de acceso de los usuarios a los sistemas y datos de la organización. El control A.9.2.1 de la norma ISO 27001, titulado "Gestión del acceso de los usuarios", establece la necesidad de controlar los derechos de acceso de los usuarios para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Este

control se centra en garantizar que los usuarios tienen los permisos de acceso adecuados y que se controlan los cambios en dichos permisos.

La oficina RE/MAX 2Mil carece de una falta de supervisión y registros de actividad, es decir, de un sistema de monitoreo y de registros. Esto significa que los eventos de seguridad relacionados con la red y los sistemas de la organización no se están registrando y analizando adecuadamente. El control A.12.4.1 de ISO 27001, titulado "Registro de eventos", establece la necesidad de registrar y revisar los eventos de seguridad para identificar y responder a incidentes de seguridad, así como para detectar actividades sospechosas o inusuales. Este control se centra en garantizar que se registran los eventos relevantes y se lleva a cabo un análisis posterior.

La empresa no ha proporcionado suficiente formación en materia de seguridad a sus empleados; esto implica que pueden no estar suficientemente informados y concienciados sobre las mejores prácticas de seguridad de la información, lo que aumenta el riesgo de cometer errores o caer en engaños que podrían comprometer la seguridad de la organización. El control A.7.2.2 de la norma ISO 27001, titulado "Concienciación, educación y formación en materia de seguridad de la información", establece la necesidad de garantizar que todos los empleados reciben una formación y concienciación adecuadas en materia de seguridad de la información. Este control se centra en garantizar que los empleados estén informados y sean conscientes de las amenazas y riesgos para la seguridad, así como de sus responsabilidades en la protección de la información.

Se ha identificado que la oficina RE/MAX 2Mil carece de políticas de seguridad claras y procedimientos documentados. Esto implica que no se han establecido directrices formales y documentadas sobre las prácticas de seguridad de la información dentro de la organización. El control A.5.1.1 de ISO 27001, titulado "Política de seguridad de la información", establece la necesidad de establecer políticas de seguridad de la información que defina los requisitos y directrices generales para la protección de la misma. Este control se centra en asegurar que la organización posea una dirección clara y un compromiso con la seguridad de la información.

Por último, la organización no dispone de un plan de gestión de parches y actualizaciones. Esto implica que los sistemas y dispositivos utilizados en la organización

pueden no estar actualizados con las últimas correcciones y parches de seguridad disponibles. El control A.12.6.1 de ISO 27001, titulado "Control técnico de la seguridad de la información o Gestión de vulnerabilidades técnicas", establece la necesidad de controlar los parches de seguridad en los sistemas de información. Este control se centra en asegurar que las organizaciones aplican regularmente actualizaciones de seguridad para mitigar las vulnerabilidades conocidas y proteger los sistemas contra ataques.

4.3 Estrategias de seguridad informática más convenientes para proteger los puntos vulnerables de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A.

Para proteger los puntos vulnerables de los sistemas de información de la franquicia inmobiliaria RE/MAX 2Mil C.A., se pueden implementar las siguientes estrategias de seguridad informática: crear un enfoque de defensa en profundidad, esta estrategia consiste en efectuar múltiples capas de seguridad para proteger los sistemas de información.

Esto incluye el uso de cortafuegos, sistemas de detección y prevención de intrusiones (IDS/IPS), antivirus, y soluciones de cifrado de datos. Disponer de varias capas de seguridad aumenta la dificultad de los atacantes para acceder a los sistemas y reduce el impacto en caso de violación de la seguridad. A su vez, establecer políticas de seguridad claras y documentadas; como ya se ha mencionado, es importante desarrollar políticas de seguridad de la información que aborden factores como el uso aceptable de los recursos, la clasificación de datos, la gestión de contraseñas y el acceso remoto. Estas políticas deben comunicarse a todos los empleados y agentes franquiciados y debe hacerse hincapié en su cumplimiento. Además, deben establecerse procedimientos documentados para apoyar y hacer cumplir estas políticas.

En otro orden, realizar evaluaciones periódicas de vulnerabilidad es aconsejable para ejecutar pruebas periódicas de la vulnerabilidad de los sistemas de la franquicia. Esto implica el uso de herramientas de escaneado de seguridad para identificar posibles puntos débiles en la infraestructura, como puertos abiertos, configuraciones inseguras o

versiones de software obsoletas. Estas evaluaciones permitirán detectar y corregir vulnerabilidades antes de que sean aprovechadas por los atacantes.

De igual forma, es esencial utilizar mecanismos de autenticación fuertes para garantizar que sólo los usuarios autorizados puedan acceder a los sistemas de información. Además de contraseñas seguras, se debe considerar la implementación de la autenticación de dos factores, como el uso de códigos generados por aplicaciones móviles o tokens físicos. Esto añade una capa adicional de seguridad al requerir algo que el usuario conoce (contraseña) y algo que el usuario tiene (dispositivo de autenticación).

Continuando con lo anterior mencionado, es importante implantar estos controles de acceso y privilegios adecuados para limitar el acceso a la información y a los recursos solo a aquellos empleados que lo necesiten para desempeñar sus funciones laborales. Esto implica, asignar funciones, permisos de forma precisa y regular, como también revisar periódicamente los privilegios concedidos. Además, deben establecerse políticas para la gestión segura de las cuentas de usuario, como la desactivación o eliminación de cuentas de empleados o agentes franquiciados que ya no trabajen en la organización.

Como última estrategia, es fundamental proporcionar formación y concienciación sobre seguridad de la información a todos los empleados y agentes franquiciados. Esto incluye educar en prácticas de seguridad como la identificación de ataques de phishing, el uso adecuado de contraseñas, la protección de datos sensibles y la detección de comportamientos sospechosos. Esta formación debe impartirse periódicamente para mantener a los empleados al día con las novedades.

PARTE V

PROPUESTA

5.1 Importancia de la Propuesta.

Se enfoca en establecer un plan de gestión de IT y llevar a cabo una auditoría de red basada en normativas internacionales. Esto permitirá asegurar el correcto funcionamiento de la red, controlar el acceso y manipulación de datos, cumpliendo con los estándares de seguridad y normativas aplicables internacionales. Al implementar estas medidas, la organización podrá fortalecer su postura de seguridad informática, proteger su información confidencial y mantener la confianza de sus clientes y socios comerciales. Si bien, es importante compartir información, también es fundamental establecer controles para garantizar que no todo el personal tenga acceso y manipulación irrestricta a los mismos. Un plan de gestión de IT adecuado asegurará que solo las personas autorizadas tengan acceso a los datos relevantes para sus responsabilidades laborales, evitando posibles filtraciones o manipulaciones indebidas de la información.

La auditoría de red basada en normativas internacionales, como la serie ISO 27000, juega un papel fundamental en la garantía de la seguridad y el cumplimiento normativo en el entorno de la red. Estas normas proporcionan un conjunto de mejores prácticas y directrices reconocidas internacionalmente para la gestión de la seguridad de la información. Gracias a esto, se pueden identificar las brechas y deficiencias existentes en la infraestructura de red y se pueden tomar medidas correctivas adecuadas para garantizar el correcto funcionamiento de la red y la protección de la información sensible.

5.2 Viabilidad de aplicación de la Propuesta.

4.2.1 Factibilidad Técnica: Fueron necesarios para la realización de este proyecto los siguientes instrumentos tecnológicos, una computadora personal con especificaciones básicas, para determinar el estado actual de las carpetas y/o archivos importantes en red de distribución en cuanto a su gestión. Y a su vez, acceso a internet para la interconexión de las distintas máquinas de la oficina.

Tabla 1: Herramientas tecnológicas para realizar la propuesta de auditoría.

Herramientas para su ejecución	Funciones
PC que cuente con mínimo 2Gb de memoria RAM, procesador de 32 bits superior a los 1.4GHz.	La PC será para determinar el estado actual de las carpetas y/o archivos en red de distribución en cuanto a su gestión.
Acceso a internet de minimo 256kbps	Acceso a internet, para interconectar las distintas PCs de la oficina.

Fuente: Elaboración propia. (2023)

Tabla 2: Costo de los instrumentos tecnológicos para ejecutar la propuesta de auditoria

Instrumentos tecnológicos	Inversión (\$)
Computadora Refurbished	120.00
Servicio de Internet Datalink (mensual)	60.00
Servicio de Internet Datalink (anual)	720.00
Total	\$840.00

Fuente: Elaboración propia. (2023)

4.2.2 Factibilidad Operativa: Esta fase se refiere al personal o mano de obra utilizada para la realización y cumplimiento de la investigación. En este trabajo se utilizó el investigador para la auditoria.

5.2.3 Factibilidad Económica

Tabla 3: Inversión de los instrumentos tecnológicos para el correcto uso de la aplicación móvil.

Instrumentos tecnológicos	Inversión (\$)
PC que cuente con mínimo 2Gb de memoria RAM, procesador de 32 bits superior a los 1.4GHz.	120.00
Servicio de Internet de 5Mbps (mensual)	20.00
Servicio de Internet de 5Mbps (anual)	240.00
Total	\$360.00

Fuente: Elaboración propia. (2023)

5.3 Objetivos de la Propuesta.

5.3.1 Objetivo General.

Realizar una auditoría de red para los procesos de seguridad de la información en la franquicia inmobiliaria RE/MAX 2Mil C.A.

5.3.2 Objetivo Específicos.

- Mejorar los protocolos de seguridad de la información en red de la franquicia inmobiliaria RE/MAX 2Mil C.A.
- Disminuir el riesgo de ataques informáticos con fines maliciosos a la red de la franquicia inmobiliaria RE/MAX 2Mil C.A.

- Concientizar al personal administrativo y agentes asociados sobre la importancia de los procesos de seguridad de la información en la red informática establecida en la franquicia inmobiliaria RE/MAX 2Mil C.A.

5.4 Representación gráfica y estructura de la Propuesta.

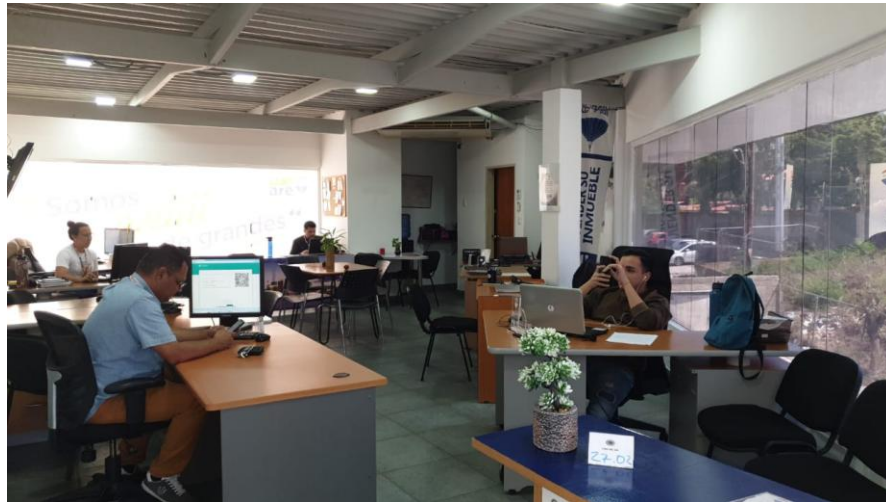
El estado actual de la seguridad informática en la franquicia inmobiliaria se caracteriza por la falta de políticas y procedimientos claros y de formación de los empleados en materia de seguridad. Además, se detectan deficiencias en el control de acceso, ausencia de supervisión y registros de actividad, falta de actualizaciones y parches del sistema. Sin embargo, tras la aplicación de las recomendaciones propuestas, la franquicia inmobiliaria experimentaría cambios significativos en su postura de seguridad informática. La aplicación de políticas y procedimientos sólidos establecerá una base sólida para la correcta protección de la información y los recursos.

Figura 1: Aspecto actual de la red de la franquicia inmobiliaria RE/MAX 2Mil.



Fuente: Elaboración propia. (2023)

Figura 2: RE/MAX 2Mil en día laboral utilizando la infraestructura de la oficina.



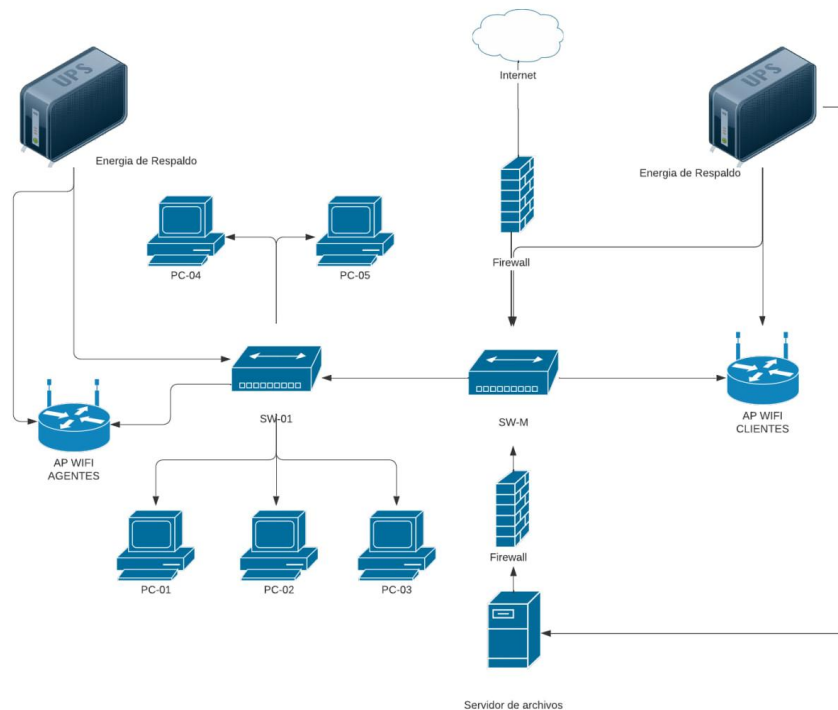
Fuente: Elaboración propia. (2023)

Figura 3: Cableado de la oficina RE/MAX 2Mil.



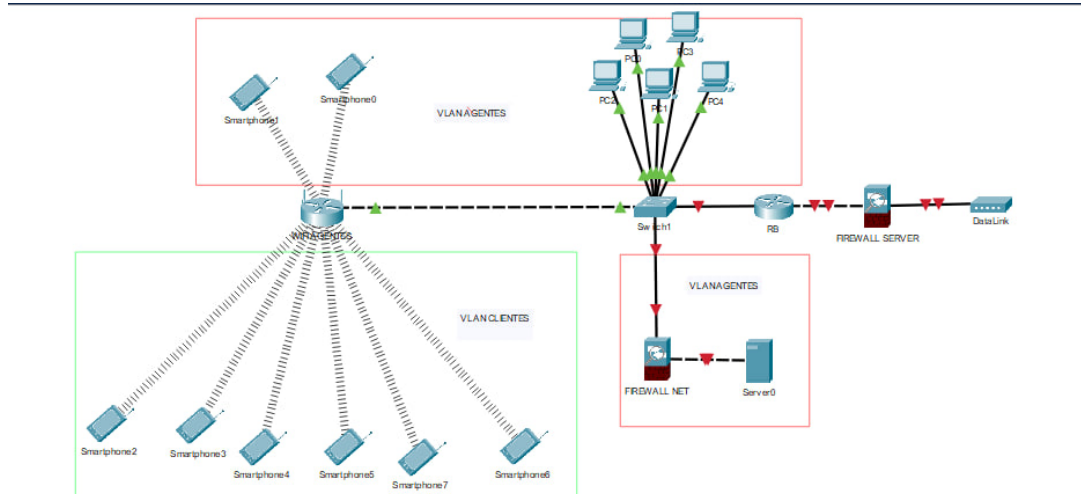
Fuente: Elaboración propia. (2023)

Figura 4: Infraestructura recomendada para la franquicia inmobiliaria RE/MAX 2Mil



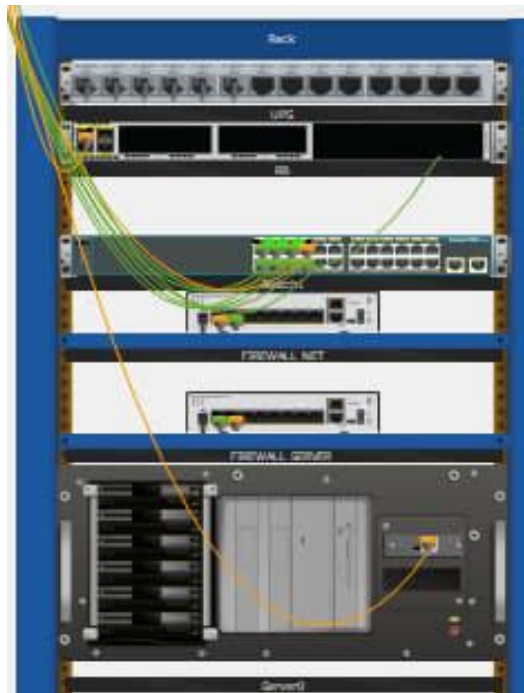
Fuente: Elaboración propia. (2023)

Figura 5: Infraestructura recomendada en software Cisco Packet Tracer



Fuente: Elaboración propia. (2023)

Figura 6: Representación de Infraestructura en software Cisco Packet Tracer



Fuente: Elaboración propia. (2023)

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Este trabajo de investigación ha explorado la importancia de la seguridad informática en la protección de los sistemas de información en el contexto de una franquicia inmobiliaria. Aunque en la actualidad no existe un marco integral de seguridad de red implantado en la organización objeto de estudio, es fundamental estar preparado y responder de forma ágil a las amenazas y vulnerabilidades que surgen en el día a día de las operaciones. A lo largo del estudio, se ha analizado la necesidad de implantar medidas de seguridad física y de red para garantizar la confidencialidad, integridad y disponibilidad de la información y los activos en la organización.

A través del uso de herramientas de recolección de datos, el investigador ha observado una falta de metodología para establecer una adecuada segregación de funciones dentro de las diferentes áreas o puestos de trabajo de acuerdo a las normativas internacionales, en este caso ISO. Esta deficiencia, limita la capacidad de hacer frente de manera eficaz y eficiente las amenazas y vulnerabilidades, lo que se traduce en un aumento de los riesgos para la franquicia inmobiliaria. Por lo tanto, es fundamental implementar controles adecuados para evitar la materialización de los riesgos, sobre todo considerando que la información que se maneja en este entorno constituye la base del desempeño de la organización.

Dicho lo anterior, como resultado de esta investigación se han propuesto estrategias y recomendaciones específicas para hacer frente a estas vulnerabilidades. Entre ellas se encuentran la implantación de una arquitectura de red segmentada, políticas de gestión de accesos y privilegios, sistemas de seguridad de red y monitorización de eventos, programas de formación en seguridad de la información, desarrollo de políticas y procedimientos de seguridad documentados en la franquicia inmobiliaria. Es fundamental que dicha organización reconozca la importancia de aplicar estas estrategias y tomar medidas proactivas para reforzar la seguridad de sus sistemas de información. Hacerlo,

ayudará a mitigar los riesgos de posibles amenazas y vulnerabilidades, proteger los datos sensibles y mantener la confianza de los clientes.

Recomendaciones

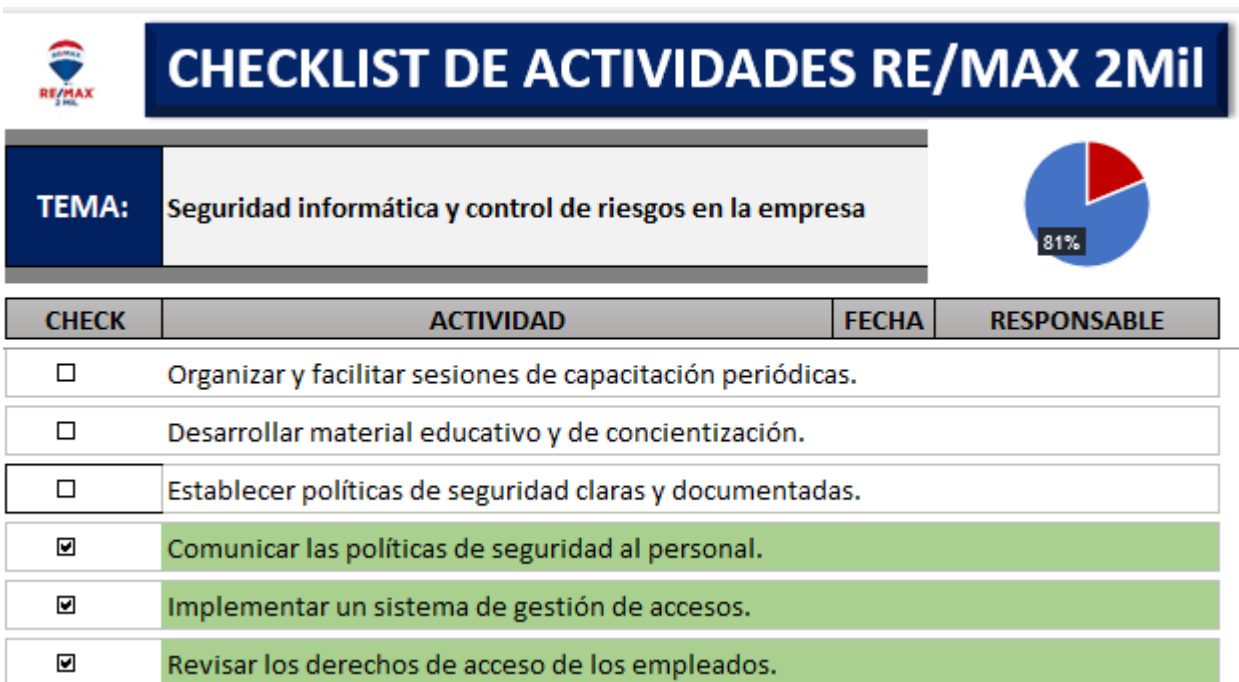
Como conclusión del trabajo de investigación sobre la estructura de red de la inmobiliaria RE/MAX 2Mil, refuerzan la seguridad y protección de los sistemas de información y garantizan la confidencialidad, integridad y disponibilidad de los datos y activos de la organización. Por lo tanto, se hacen las siguientes recomendaciones:

1. Se sugiere establecer VLAN para separar las redes de clientes y empleados, lo que puede mejorar la seguridad y el control de acceso a los recursos de la red.
2. Para proteger la red de amenazas externas, es importante instalar cortafuegos en los puntos de entrada y salida de la red. También hay que establecer políticas de seguridad para controlar el tráfico y evitar accesos no autorizados.
3. Para reforzar la seguridad de las cuentas de usuario, se recomienda implantar métodos de autenticación de dos factores, como el uso de contraseñas y códigos de autenticación enviados a dispositivos móviles.
4. Debe desarrollarse una política clara para controlar los derechos de acceso de los empleados a los recursos de la red. De acuerdo con el principio de "mínimo privilegio", es importante que sólo se concedan las autorizaciones necesarias para el desempeño de sus funciones.
5. Se recomienda utilizar una solución de seguridad de red y supervisión de eventos para registrar y analizar la actividad de la red. Esto permite identificar posibles amenazas y vulnerabilidades y actuar rápidamente en consecuencia.

6. Formar y concienciar a todos los empleados sobre la seguridad de la información. Esto incluye la identificación de ataques de phishing, el uso adecuado de contraseñas y la protección de datos sensibles.

Además, el investigador proporciona una lista de actividades, que es una guía integral para que el personal correspondiente pueda cuidar y mantener la seguridad de la red en la franquicia inmobiliaria. Estas actividades abarcan tres áreas clave: el ámbito humano, lógico y físico, y se centran en acciones específicas que se deben llevar a cabo para proteger los sistemas de información y los activos de la oficina. Para facilitar el seguimiento y la implementación de estas actividades, se diseñó una hoja de cálculo en Microsoft Excel. A continuación, presento una forma de organizar la información en un formato interactivo:

Gráfico 12. Checklist de actividades RE/MAX 2Mil



CHECK	ACTIVIDAD	FECHA	RESPONSABLE
<input type="checkbox"/>	Organizar y facilitar sesiones de capacitación periódicas.		
<input type="checkbox"/>	Desarrollar material educativo y de concientización.		
<input type="checkbox"/>	Establecer políticas de seguridad claras y documentadas.		
<input checked="" type="checkbox"/>	Comunicar las políticas de seguridad al personal.		
<input checked="" type="checkbox"/>	Implementar un sistema de gestión de accesos.		
<input checked="" type="checkbox"/>	Revisar los derechos de acceso de los empleados.		

Fuente: Elaboración propia. (2023)

Con esta estructura en Microsoft Excel, se realiza un seguimiento interactivo de las actividades de seguridad de la red. Se puede marcar progreso de cada actividad, establecer fechas límite y asignar responsables. Se recomienda a la organización actualizar y revisar regularmente esta hoja de cálculo para asegurarse de que todas las

actividades se estén llevando a cabo de manera oportuna y efectiva. Esto proporcionará una herramienta práctica para realizar un chequeo de las acciones de seguridad y mantener un registro de su cumplimiento en un determinado periodo de tiempo.

REFERENCIAS BIBLIOGRÁFICAS

A. (2022, 12 abril). *Redes cableadas e inalámbricas: todas las diferencias*. CompuMax.
<https://compumax.ec/redes-cableadas-e-inalambricas-todas-las-diferencias/>

A. (2023, 24 enero). *Redes alámbricas - SOTEIN empresa de mantenimiento de redes*. SOTEIN. <https://sotein.com.co/redes-alambricas/>

Ley especial contra los delitos informáticos. Asamblea Nacional (2001). Caracas, Venezuela.

Ley Orgánica de Telecomunicaciones. Asamblea Nacional (2011). Caracas, Venezuela.

Ley sobre el derecho de autor. Congreso de la República (1993). Caracas, Venezuela.

Ley sobre protección a la privacidad de las comunicaciones. Congreso de la República (1991). Caracas, Venezuela.

AUDITORIA AL CENTRO DE DATOS DE LA UNIVERSIDAD BENITO JUAREZ. (2011, marzo). tesis.ipn.mx. Recuperado 24 de marzo de 2023, de <https://tesis.ipn.mx/bitstream/handle/123456789/13165/ice341..pdf?sequence=1&isAllowed=y>

AUDITORIA DE EMPRESAS EN EL ÁREA DE TELECOMUNICACIONES. (2005, abril). <http://biblioteca.usac.edu.gt/>. Recuperado 24 de marzo de 2023, de http://biblioteca.usac.edu.gt/tesis/08/08_0249_CS.pdf

AUDITORIA DE RED LOCAL MEDIANTE UN DISPOSITIVO AUTÓNOMO. (2021, junio). openaccess.uoc.edu. Recuperado 24 de marzo de 2023, de <https://openaccess.uoc.edu/bitstream/10609/132570/8/israeltorresTFG0621memoria.pdf>

Capitulo III —. (2013b, enero 22). Metodología de la Investigación. <https://bianneygiraldo77.wordpress.com/category/capitulo-iii/> *Capitulo III - Marco Metodológico*. (s. f.). virtual.urbe.edu.

MANUAL DE AUDITORIA DE LA RED FÍSICA Y LÓGICA EN LA DIRECCIÓN NIC.NI. (2016). [TESIS DE PREGRADO]. UNIVERSIDAD NACIONAL DE INGENIERÍA RECINTO UNIVERSITARIO «SIMÓN BOLÍVAR».

MODELO DE MADUREZ DE SEGURIDAD DE LA INFORMACIÓN PARA EL MONITOREO Y ANÁLISIS DEL TRÁFICO DE REDES EN LA ADMINISTRACIÓN PÚBLICA NACIONAL DE VENEZUELA. (2016, junio). biblioteca2.ucab.edu.ve. Recuperado 24 de marzo de 2023, de <http://biblioteca2.ucab.edu.ve/anexos/biblioteca/marc/texto/AAT4688.pdf>

SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN COMO MECANISMO PARA LA ACTUALIZACIÓN DE LAS MEDIDAS DE PROTECCIÓN DE DEPARTAMENTO DE INFORMÁTICA DE UNA UNIVERSIDAD PÚBLICA. (2015, 14 octubre). mriuc.bc.uc.edu.ve. Recuperado 24 de marzo de 2023, de <http://mriuc.bc.uc.edu.ve/bitstream/handle/123456789/5819/jgomez.pdf?sequence=1>

Dynamic Authentication-Based Secure Access to Test Infrastructure. (2020, 1 diciembre). hal.science. Recuperado 9 de febrero de 2023, de <https://hal.science/hal-02887467/document>

Wireless LAN Security: What Hackers Know That You Don't. (2014, abril). s26142.pcdn.co. Recuperado 5 de febrero de 2023, de https://s26142.pcdn.co/wp-content/uploads/2014/04/What-Hackers-Know_id42.pdf

Auditoria de sistemas una visión práctica. (2007). repositorio.unal.edu.co. Recuperado 14 de febrero de 2023, de <https://repositorio.unal.edu.co/handle/unal/60273>

Process-mining-enabled audit of information systems: Methodology and an application. (2018, 7 junio). Recuperado 11 de febrero de 2023, de <https://www.sciencedirect.com/science/article/abs/pii/S0957417418303300>

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES. (2018, octubre). 3ciencias.com. Recuperado 17 de febrero de 2023, de <https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informatica.pdf>

J. Voas, N. Kshetri and J. F. DeFranco, "Scarcity and Global Insecurity: The Semiconductor Shortage," in *IT Professional*, vol. 23, no. 5, pp. 78-82, 1 Sept.-Oct. 2021, doi: 10.1109/MITP.2021.3105248.

El Informe sobre amenazas de seguridad en la nube de Symantec CSTR 2019. (s. f.). Symantec Enterprise Blogs. <https://symantec-enterprise-blogs.security.com/blogs/america-latina/informe-de-amenazas-de-seguridad-en-la-nube>

ISTR 2019: Internet of Things Cyber Attacks Grow More Diverse. (s. f.). Symantec Enterprise Blogs. <https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/istr-2019-internet-things-cyber-attacks-grow-more-diverse>

U., & Completo, V. M. P. (s. f.). *redes alámbricas.* <http://hrpphernanpolopacheco.blogspot.com/p/redes-alambricas.html>

Razo, C. (2002). *Auditoria en Sistemas Computacionales.* In Pearson Educación eBooks. Pearson Educación. <http://up-rid2.up.ac.pa:8080/xmlui/handle/123456789/1352?show=full>

- Alzate, A. T. (2007). Auditoria de sistemas una visión práctica. <https://repositorio.unal.edu.co/bitstream/handle/unal/60273/9589322662.pdf?sequence=1&isAllowed=y>
- Álvarez, L. (2005). "SEGURIDAD EN INFORMÁTICA (AUDITORÍA DE SISTEMAS)." UNIVERSIDAD IBEROAMERICANA. https://ri.iberomx/bitstream/handle/iberomx/1010/014663_s.pdf?sequence=1&isAllowed=y
- Bruce, W. (2016). Audit and networking security. https://www.researchgate.net/publication/303698398_Audit_and_networking_security
- Kearns, M. (2004). Economics, Computer Science, and Policy. University of Pennsylvania. <https://www.cis.upenn.edu/~mkearns/teaching/NetworkedLife/ist.pdf>
- Kshetri, N., & Voas, J. (2017). Hacking Power Grids: A Current Problem. IEEE Computer, 50(12), 91–95. <https://doi.org/10.1109/mc.2017.4451203>
- García, J. Universidad Autónoma del Estado de Hidalgo. (2014). El marco teórico. Edu.Mx. Recuperado el 28 de abril de 2023, de <https://www.uaeh.edu.mx/scige/boletin/prepa4/n2/m4.html>
- Hernández, E. y Nadir, K. (2018). Edu.ni. Recuperado el 28 de abril de 2023, de <https://ribuni.uni.edu.ni/2281/1/93017.pdf>
- Ramírez, M. (2011). Ipn.mx. Recuperado el 28 de abril de 2023, de <https://tesis.ipn.mx/bitstream/handle/123456789/13165/ice341..pdf?sequence=1&isAllowed=y>
- Mayol, R. (2006). MODELO PARA LA AUDITORÍA DE LA SEGURIDAD INFORMÁTICA EN LA RED. Mendillo.info. Recuperado el 28 de abril de 2023, de <http://mendillo.info/seguridad/tesis/Mayol.pdf>
- Axelos. (2019). ITIL® 4: Directrices de la Fundación. TSO (The Stationery Office).

- Hernando, I. (2016, marzo 31). GOBERNANZA DE TI: ESENCIAL PARA LA TOMA DE DECISIONES. Inycom.es. <https://trends.inycom.es/gobernanza-ti-esencial-la-toma-decisiones/>
- Saffirio, M (2006). Gobernabilidad TI – IT Governance. Tecnologías de la Información y Procesos de Negocios. <https://msaffirio.com/2006/07/09/gobernabilidad-ti-it-governance/>
- da Silva, D. (2021, agosto 10). Qué es ITIL y para qué sirve: glosario explicativo. Zendesk MX. <https://www.zendesk.com.mx/blog/itil-que-es-para-que-sirve/>
- Mann, S. (s/f) ITIL: Qué es, cómo funciona y cómo implementarlo. Freshworks.com. Recuperado el 29 de abril de 2023, de <https://www.freshworks.com/es/freshservice/itil/que-es-itil/>
- Piattini & Del Peso. (2001). Auditoría Informática: Un enfoque práctico. Edu.bo. Recuperado el 29 de abril de 2023, de <http://cotana.informatica.edu.bo/downloads/Id-Auditoria-informatica-un-enfoque-practico-Mario-Piattini-pdf.pdf>
- Canales Mena, E. (2006). Auditoría física en la Facultad de Ingeniería Química. Tesis inédita de Ingeniería, Universidad Nacional de Ingeniería, Managua.
- Tanenbaum, A. (2003). Redes de computadoras (Cuarta ed.). (E. Núñez Ramos, Ed.) México D.F., México: Pearson Educación.
- Tanarro, G. (2010). Auditoría y Diseño de red en un entorno universitario. Core.ac.uk. Recuperado el 29 de abril de 2023, de <https://core.ac.uk/download/30043931.pdf>
- Mendoza, A. (2015). Conoce los tipos de auditorías de redes y qué puede revisar cada una. WeLiveSecurity. <https://www.welivesecurity.com/la-es/2015/04/20/auditorias-de-redes/>
- Echenique, G. (2002). Auditoría en Informática (Segunda ed.). México D.F., México:

McGraw Hill.

Maiwald, E. (2005). *Fundamentos de seguridad de redes (Segunda ed.)*. México D.F., México: McGraw Hill.

Wangler, B. (2005). *Information Systems Engineering: What Is It?* Researchgate.net.
https://www.researchgate.net/publication/220921360_Information_Systems_Engineering_What_Is_It

Whitten, J., Bentley, L. y Dittman, K. (2004). *System analysis y design methods*. Editoroal Mc. Graw Hill

Gómez, A. (2006). *Enciclopedia de la seguridad informática*, RA-MA, España.

Kissel, R. (2012). *Glossary of Key Information Security Terms*, National Institute of Standardand Technology. doi.org/10.6028/ NIST.IR. 7298.

Cordovilla, A. y Sigcho, O. (2020). *Ciencias de la computación Artículo de investigación*. 6, 835–846.

Guisao, J. S., & Toro Rendon, J. C. (2014). *Introducción Metodología para la detección de vulnerabilidades de redes de datos*. 63–67.

ManageEngine. (s/f). *Escaneo de vulnerabilidades*. Manageengine.com. Recuperado el 30 de abril de 2023, de <https://www.manageengine.com/latam/vulnerability-management/analisis-de-vulnerabilidades.html>

Latto, N. (2020). *Exploits: todo lo que debe saber*. Exploits: todo lo que debe saber; Avast. <https://www.avast.com/es-es/c-exploits>

Albors, J. (2022, diciembre 22). *Qué es un exploit: la llave para aprovechar una vulnerabilidad*. WeLiveSecurity. <https://www.welivesecurity.com/la-es/2022/12/22/exploits-que-son-como-funcionan/>

- Portolan, M. (2020). A comprehensive end-to-end solution for a secure and dynamic mixed-signal 1687 system. *2020 IEEE 26th International Symposium on On-Line Testing and Robust System Design (IOLTS)*.
- Juntadeandalucia.es (s/f). Conceptos de seguridad en aplicaciones WEB. Recuperado el 30 de abril de 2023, de <https://www.juntadeandalucia.es/servicios/madeja/contenido/recurso/212>
- Florencia, U. (2009). Definición de Ataque. DefinicionABC. Recuperado el 30 de abril de 2023, de <https://www.definicionabc.com/general/ataque.php>
- Tarazona, T. (2007). Holdings Metarevistas.org Amenazas informáticas y seguridad de la información. Recuperado el 1 de mayo de 2023, de <https://metarevistas.org/Record/oai:revistas.uexternado.edu.co:articleojs-965>
- Mieres, A. J. (2009). Debilidades de seguridad comúnmente explotadas. Evilfingers.com. Recuperado el 1 de mayo de 2023, de https://www.evilfingers.com/publications/white_AR/01_Atques_informaticos.pdf
- Ruben, A. (2018). Qué es la dirección MAC de tu ordenador o móvil y para qué sirve. Computer Hoy. <https://computerhoy.com/reportajes/tecnologia/direccion-mac-ordenador-movil-sirve-317181>
- Patrizio, A. (2019). ¿Qué es una dirección IP? ¿Qué es una dirección IP?; Avast. <https://www.avast.com/es-es/c-what-is-an-ip-address>
- Burke, J., Irei, A., & Chai, W. (2021, mayo 31). Ethernet. ComputerWeekly.es; TechTarget. <https://www.computerweekly.com/es/definicion/Ethernet>
- Guillén, J. (2017). Introducción al pentesting. Diposit.ub.edu. Recuperado el 1 de mayo de 2023, de <https://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf>

- Turolde, T. (2015). *DEFINICION DE NODO, PROTOCOLO, TCP/IP*. prezi.com.
Recuperado el 1 de mayo de 2023, de <https://prezi.com/ibzhvl-qmtfe/definicion-de-nodo-protocolo-tcpip/>
- Proaño, F (2015). *DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN*. Edu.ec.
Recuperado el 1 de mayo de 2023, de <https://repositorio.espe.edu.ec/bitstream/21000/11218/1/T-ESPE-048964.pdf>
- Corvo, H. (2019) *REESTRUCTURACIÓN DE LA RED DE DATOS* Recuperado el 1 de mayo de 2023, de <https://repository.ucc.edu.co/server/api/core/bitstreams/f7f98a60-794e-4b05-a9c1-8acdc5b27b0e/content>
- Marchionni, A. (2011). Wordpress.com. Recuperado el 1 de mayo de 2023, de <https://clasesdeseguridadinformatica.files.wordpress.com/2014/03/administrador-de-servidores.pdf>
- Borges, S. (2020). *¿Qué es un Servidor local? Ventajas, desventajas e instalación*. Infranetworking. <https://blog.infranetworking.com/servidor-local/>
- Tamayo y Tamayo, Mario (2003). *El Proceso de La Investigación Científica*. Scribd.
Recuperado el 1 de mayo de 2023, de <https://es.scribd.com/doc/12235974/Tamayo-y-Tamayo-Mario-El-Proceso-de-la-Investigacion-Cientifica>
- Ostec. (2005). *ISO 27002: Buenas prácticas para gestión de la seguridad de la información*. Recuperado el 28 de septiembre de 2021 de <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/>.
- EEE. (2019, septiembre 5). *Cómo gestionar los controles de acceso según ISO 27001*. Escuela Europea de Excelencia.
<https://www.escuelaeuropeaexcelencia.com/2019/09/como-gestionar-los-controles-de-acceso-segun-iso-27001/>