UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA

PROCESO DE TITULACIÓN

NOVIEMBRE 2021 – ABRIL 2022

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TITULO DE

INGENIERO(A) EN SISTEMAS DE INFORMACIÓN

TEMA:

VULNERABILIDADES EN EL SISTEMA DE INFORMACION EN EL SOPORTE DE INVENTARIO DEL DISTRIBUIDOR MAYORISTA DE PRODUCTOS DE FERRETERIA ¨FERREQUIM SA¨

EGRESADA(O):

JOMIRA KATHERINE BERRUZ GORDILLO

TUTOR:

ING. HUGO JAVIER GUERRERO TORRES.

AÑO 2022

CONTENIDO

CONTENIDO 1
PLANTEAMIENTO DE PROBLEMAS 3
JUSTIFICACIÓN 5
OBJETIVOS 6
Objetivo general 6
Objetivos específicos 6
LÍNEAS DE INVESTIGACIÓN 7
MARCO CONCEPTUAL 8
La información 9
Tipos de amenazas 9
Seguridad de la información 10
Funciones de los empleados 10
Redes informáticas 11
Elemento de gestión de la seguridad de los sistemas de información 11
Identificación de todos los activos del sistema 12
Identificación de amenazas de los activos 12
Identificación de vulnerabilidades 13
Identificación de impactos 14
Identificación de riesgo 14
Identificación de riesgos residuales 15
Aplicación de salvaguardas 15
Identificación de las limitaciones de aplicación de la seguridad 16
Análisis de vulnerabilidad 16
Matriz de riesgos 16
MARCO METODOLÓGICO 19
Diseño de investigación 19
RESULTADOS 23
DISCUSIÓN DE RESULTADOS 29
CONCLUSIONES 31
RECOMENDACIÓNES 33
REFERENCIAS 34
ANEXO 35

Anexo 1: organigrama de la empresa 35
Anexo 2: entrevista 35

PLANTEAMIENTO DE PROBLEMAS

La empresa FERREQUIM SA se ubica en la ciudad de Guayaquil y se dedica a la importación y comercialización de artículos de ferretería, accesorios para mobiliario y para la construcción.

La empresa al ser catalogada pyme cuenta con un sistema de información conformado por el software contable LUMBRERA® que realiza las actividades de facturación electrónica, inventario de clientes - proveedores, registro de instituciones bancarias con las que se trabajara, emisión de roles de pagos, registro de presupuestos. Existen otros componentes dentro de la empresa como: la infraestructura de red, los equipos informáticos y el personal. Podemos resaltar varios aspectos importantes del software utilizado por la empresa, que no permiten que este cumpla con su finalidad en un 100%, entre las observaciones se destaca que la empresa maneja grandes volúmenes de información debido a las ventas que realiza, la vulnerabilidad de esta información se presenta al no contar con mecanismos adecuados para salvaguardarla de posibles efectos negativos poniendo en riesgo su seguridad.

El sistema cuenta con el software contable para llevar las gestiones empresariales de manera ordenada, en el software mencionado se han detectado algunas anomalías como congelamiento del mismo el cual no permite realizar las actividades de forma continua debido a que se tiene que esperar a que el programa vuelva a funcionar y el otro problema detectado es la realización de transacciones erróneas. Estas se muestran al momento de hacer facturaciones y posteriormente emitir el comprobante de retención por el proceso realizado este no calculaba bien

el porcentaje alterando la caja de la empresa porque daba valores faltantes o sobrantes en algunos casos, estos problemas presentados generan desorden, por lo que es necesario hacer un análisis del software para aportar una futura solución al problema que pueda prevenir paralizaciones de las actividades y evitar pérdidas en la empresa.

La empresa cuenta con conectividad a internet, pero el problema consiste en la antigüedad de sus equipos, los cuales no manejan un protocolo de seguridad actual, lo cual es necesario contar con una buena estructura de red, siendo elementos críticos al momento de implementar un sistema de información, dentro de la infraestructura de FERREQUIM SA no posee un software para detectar intrusos. La empresa no cuenta con sucursales, esta tiene un solo punto de venta, en la oficina matriz, desde ahí, se operan las actividades las cuales se realizan a través de internet, entre ellas están las interacciones con los usuarios minoristas y mayoristas mediante la página web de la empresa y con los proveedores por medio del software. Sin una buena conectividad, estas acciones se verían afectadas ya que no se lograría una buena comunicación.

JUSTIFICACIÓN

El presente proyecto se enfoca sobre como las vulnerabilidades o amenazas de un sistema de información puede afectar el funcionamiento de una empresa y poner en riesgo la seguridad de la misma, el sistema de inventario que maneja la empresa contiene la mayor cantidad de datos importante por lo que estas falencias afecta de manera directa a la información dando como resultado valores erróneos en el cierre de caja, con este proyecto se pretende demostrar las soluciones a las vulnerabilidades con las que cuenta la empresa FERREQUIM SA.

La realización de este proyecto permitirá, examinar los procesos realizados en el sistema de información de la empresa FERREQUIM SA, para luego estimar las vulnerabilidades seleccionando normativas y procedimientos adecuados, para preservar la integridad de la información en la comprobación de inventario.

OBJETIVOS

Objetivo general

- Evaluar las vulnerabilidades o riesgos en el sistema de información de la ferretería FERREQUIM S.A. en el soporte de inventarios.

Objetivos específicos

- Examinar los procesos realizados en el Sistema de Información de la empresa FERREQUIM S.A
- Estimar la vulnerabilidad de los procesos que manejan datos del sistema de información de la empresa FERREQUIM S.A
- Seleccionar normativas y procedimientos adecuados para mantener la integridad de la información en el control de inventarios

LÍNEAS DE INVESTIGACIÓN

Este caso de estudio se realizará siguiendo los lineamientos determinados en la línea de investigación de Sistemas de información y comunicación, emprendimiento e innovación, y en la sub línea de investigación que comprende las redes y tecnologías inteligentes de software y hardware, mediante un análisis de amenazas y vulnerabilidades a los sistemas de información de la empresa ¨FERREQUIM SA¨ de la ciudad de Guayaquil.

Actualmente en las empresas los sistemas de información son uno de los componentes más importantes este abarca una serie de procesos para el buen uso de la información además de apoyar en la organización y en la toma de decisiones, por lo que es necesario que este conjunto de elementos cumpla con los requerimientos que se necesitan para lograr el éxito en la organización. estas herramientas al usar internet como medio de transmisión, están expuestas a vulnerabilidades inminentes

.

MARCO CONCEPTUAL

Define (De Pablos Heredero, López Hermoso Agius, Martín-Romo Romero, & Medina Salgado, 2019) Un sistema de información empresarial (SI) es un conjunto de recursos técnicos, humanos y económicos interconectados dinámicamente que se organizan para satisfacer las necesidades de información de una organización empresarial para administrar y tomar decisiones.

Un sistema de información consta de elementos o componentes básicos como se muestra a continuación.

- **La información,** Es decir, cualquier cosa que el sistema capture, almacene, procese y entregue.
- **Las personas,** Quién es la persona que ingresa y utiliza la información en el sistema.
- **Los equipos de tratamiento de la información e interacción con los usuarios,** hardware, software y redes de comunicación.
- **Las normas y/o técnicas de trabajo,** El método utilizado por personas y tecnología para sus actividades.

La información

Según (De Pablo Heredero, López Hermoso Agius, Martín-Romero, y Medina Salgado, 2019) La información dentro de las empresas es uno de los activos más importantes por lo tanto esta debe contar con métodos actualizados para mantenerla segura y en muchos casos no se le da la importancia debida, ya que los gerentes piensan que porque sus empresas no son grandes no existen riesgos.

Tipos de amenazas

Como opina (Romero, 2018) Hay peligros que son difíciles de controlarlos, como los desastres naturales, pero deben tenerse en cuenta al calcular los riesgos, una persona puede eliminar accidentalmente la información del servidor o puede enviar un correo electrónico con secretos de información para el destinatario incorrecto, en el destinatario incorrecto mismo lugar. Las compañías de recursos informáticos pueden dañarse para uso, inundaciones, errores eléctricos, entre otros.

Las amenazas voluntarias son ataques intencionales por parte de actores dentro o fuera de la organización, los actores internos pueden ser, por ejemplo, empleados insatisfechos o ex empleados no recuperados para acceder a datos, mientras que los actores externos pueden ser competencia desleal, activistas, terroristas, ciberdelincuentes.

Seguridad de la información

Como afirma (Alano, 2021) Seguridad de la información, nos referimos ante todo a la integridad, disponibilidad y confidencialidad de la información. El objetivo de la seguridad es proteger estos tres pilares.

En el mundo corporativo, se utiliza para proteger los datos recopilados y administrados por las organizaciones. La información es un activo vital para una empresa, y la gestión eficaz de su procesamiento, almacenamiento y transmisión es fundamental.

El riesgo de información surge cuando se juntan dos factores: amenazas y vulnerabilidades. Los riesgos y las vulnerabilidades están íntimamente relacionados y sin su existencia no habría consecuencias. Las amenazas deben aprovechar las vulnerabilidades y pueden provenir de cualquier parte del entorno de la organización, tanto interna como externa. Según (Tarazona, 2007)

Funciones de los empleados

Como afirma (Gomez, 2014) Siempre debe definir las funciones y responsabilidades de cualquier otra persona que tenga acceso a los servicios del sistema de información y datos de la organización. Cada organización debe tomar las medidas necesarias para conocer las normas de seguridad que inciden en el desarrollo de la usabilidad y el cumplimiento de los usuarios de las herramientas y servicios informáticos.

Redes informáticas

Según (Lederkremer, 2019) Las redes informáticas nos permiten acceder a muchos terminales, servidores y centros de almacenamiento de información interconectados, así como manipular la información de forma remota. El concepto de seguridad es que podemos confiar en que la información que almacenamos o transmitimos solo está disponible para personas autorizadas y siempre puede ser registrada, auditada e identificada a medida que implementamos la seguridad. En las redes informáticas, debemos asegurarnos de que ambos tipos de transporte (por ejemplo, almacenamiento) son fiables.

Elemento de gestión de la seguridad de los sistemas de información

Según Javier Areitio Bertolin (2008), afirma que el proceso de gestión de la seguridad del sistema de TI incluye varios elementos, tales como:

- Identificación de todos los activos
- Identificación de las amenazas a los activos
- Identificación de vulnerabilidades
- Identificación de impactos
- Identificación de riesgos
- Aplicación de salvaguardas
- Identificación de riesgos residuales
- Limitaciones

Identificación de todos los activos del sistema

Los activos son elementos relacionados con el entorno, como personas, edificios, instalaciones, equipos o suministros, elementos relacionados con los sistemas TIC, como hardware, software, elementos TIC; relacionados con la información, relacionados con la función de la organización, tales como: capacidad para proporcionar servicios, capacidad para crear productos, activos intangibles como la imagen de la organización, reputación, conocimiento El conocimiento obtenido, la propiedad no protegida requiere una evaluación de riego aceptable. Las características de los activos incluyen la valoración interna cuantitativa y/o la posible pérdida de confidencialidad, integridad, disponibilidad y autenticidad. (BERTOLIN, 2008)

Identificación de amenazas de los activos

Los peligros pueden conducir a eventos inesperados que pueden provocar varios daños o pérdidas a la organización. Estas pérdidas pueden provenir de ataques directos o indirectos a los sistemas de información, TIC o procesos manuales. Los ataques toman principalmente la forma de divulgación, destrucción, modificación no autorizada, no disponibilidad o pérdida de información.

Las amenazas deben explotar la vulnerabilidad de los activos, tener estadísticas relacionadas con amenazas ambientales como inundaciones, rayos y terremotos para usar en el proceso de evaluación. Las amenazas pueden provenir del interior de la organización, como el sabotaje de los empleados, el robo de contraseñas por parte de ladrones (espías), el acceso no autorizado a Internet o DoS (denegación de servicio).

Los daños causados por las amenazas pueden ser temporales o permanentes y pueden estar relacionados con la gravedad, así como con otros fenómenos. Por ejemplo, los terremotos pueden tener diferente gravedad según la escala de Richter, y los virus pueden causar diferentes daños según su comportamiento. (BERTOLIN, 2008)

Entre las características más relevantes de una amenaza se encuentran las siguientes:

- El origen puede ser interno o externo
- La motivación, como son las ventajas competitivas, los beneficios económicos etc.
- La frecuencia o periodicidad de los ataques
- La severidad, dependiendo si es o no irreversible

Identificación de vulnerabilidades

La vulnerabilidad en sí no causa ningún daño; es simplemente una condición o conjunto de condiciones que pueden permitir que un recurso se vea afectado por una amenaza.

Puede haber vulnerabilidades en un sistema u organización que ninguna amenaza importante pueda explotar, por lo que todas las vulnerabilidades de amenazas deben abordarse de inmediato.

La evaluación de vulnerabilidades es el examen de las debilidades del sistema que pueden ser explotadas por amenazas identificadas, y el análisis debe tener en cuenta el entorno existente y las características de seguridad. (BERTOLIN, 2008)

Identificación de impactos

El impacto es la consecuencia de una amenaza a los activos, como la destrucción de algunos activos, amenazas a la integridad de los sistemas de información, pérdida de autenticidad, seguridad o disponibilidad.

Una posible consecuencia directa de un impacto cuantitativo o cualitativo es la pérdida financiera, la pérdida de participación de mercado o un impacto negativo en la imagen de la organización. (BERTOLIN, 2008)

Identificación de riesgo

El riesgo es la posibilidad de que un impacto afecte un activo, un dominio (o conjunto de activos) o una organización completa. Este efecto se produce porque la amenaza explota el agujero de seguridad provocando pérdida o extravío de datos.

Un entorno de riesgo es un entorno en el que una amenaza particular o un conjunto de amenazas pueden explotar una vulnerabilidad particular o un conjunto de vulnerabilidades para causar daño o pérdida de recursos.

Cualquier cambio en los activos, amenazas, vulnerabilidades y seguridad puede tener un impacto significativo en el riesgo. Detecte o comprenda rápidamente los cambios en su entorno o sistemas para ayudarlo a tomar las decisiones correctas. (BERTOLIN, 2008)

Identificación de riesgos residuales

Esto incluye comprender qué riesgos quedan después del proceso de mitigación. A menudo, estas amenazas solo se mitigan parcialmente con medidas de seguridad.

Esto significa que aún existen riesgos y debemos analizar si son aceptables como parte del proceso de equilibrar las necesidades de seguridad con las necesidades de la organización. Recuerde, cuanto mayor sea la protección, mayor será el costo.

La gerencia de la empresa debe comprender todas las demás amenazas, incluido el impacto y la probabilidad de un ataque. (BERTOLIN, 2008)

Aplicación de salvaguardas

La seguridad, también conocida como contramedidas o controles, son programas o dispositivos físicos o lógicos que previenen amenazas, reducen las vulnerabilidades de seguridad, reducen el impacto de eventos imprevistos y facilitan la recuperación. (BERTOLIN, 2008)

Identificación de las limitaciones de aplicación de la seguridad

Incluye una comprensión de las restricciones en el entorno que afectan las contramedidas y los sistemas de seguridad, especialmente los riesgos y las amenazas a la seguridad. Estos límites son establecidos y aprobados por la dirección de la organización y dependen del entorno en el que se trabaja. Pueden ser organizativos, financieros, ambientales, de personas, de tiempo, legales, técnicos, etc. (BERTOLIN, 2008)

Análisis de vulnerabilidad

El análisis de vulnerabilidad implica identificar, clasificar y priorizar las debilidades de las aplicaciones para evaluar las amenazas predecibles y responder adecuadamente. Es un proceso de determinación de la exposición y propensión a perder un elemento o grupo de elementos frente a un peligro particular, contribuyendo a una mejor comprensión del riesgo a través de la interacción de este con el ambiente peligroso. (Cardona, s.f.)

Matriz de riesgos

Se utilizó una matriz de riesgos, que es una herramienta de gestión que puede identificar objetivamente las amenazas a la organización relacionadas con la seguridad y la salud de sus empleados. Con ella podremos mostrar las posibles amenazas que generan problemas en relación al software, hardware, datos y red de la ferretería FERREQUIM S.A. (implementandosgi, s.f.)

Figura 1

Calificación de la amenaza por colores

EVENTO	COMPORTAMIENTO	COLOR ASIGNADO	
POSIBLE	Es aquel fenómeno que puede suceder o que es factible porque no existen razones históricas y científicas para decir que esto no sucederá	VERDE	
PROBABLE	Es aquel fenómeno esperado del cual existen razones y argumentos técnicos científicos para creer que sucederá	AMARILLO	
INMINENTE	Es aquel fenómeno esperado que tiene alta probabilidad de ocurrir	ROJO	

La matriz está agrupada por diferentes escenarios de riesgo para facilitar la identificación del peligro y poder aplicar el tratamiento adecuado.

- **B (Probabilidad Baja)** - Los eventos pueden ocurrir en cualquier momento (baja probabilidad)
- **M (Probabilidad Media)** – Es probable que este evento suceda la mayor parte del tiempo.
- **A (Probabilidad Alta)** - Hay una alta probabilidad de que suceda un evento.

De igual forma, la nomenclatura utilizada para la ponderación del impacto se ha utilizado lo siguiente:

- **L (Impacto Bajo)** - En caso de incidencia, el impacto en la red será mínimo.
- **M (Impacto Medio)** - Si se produce algún incidente, las consecuencias para la red serán moderadas.

- **S (Impacto Alto)** – Si se produce este evento, las consecuencias serán muy graves, poniendo en peligro la operación.

La tabla a continuación, muestra la probabilidad y el impacto en un mapa de calor.

Tabla 1. *Mapa de Calor de Análisis de Riesgos*

		PROBABILIDAD		
		B (1)	**M (2)**	**A (3)**
IMPACTO	**L (1)**	**BL 11%**	**ML 22%**	**AL 33%**
	M (2)	**BM 22%**	**MM 44%**	**AM 66%**
	S (3)	**BS 33%**	**MS 66%**	**AS 100%**

Elaborado por: *Berruz Gordillo Jomira Katherine*

.

MARCO METODOLÓGICO

El anteproyecto se realiza a través de lineamientos descriptivos, lineamientos similares que se encargan de citar y precisar el contexto que se muestra en la disputa, y definir las características, antecedentes y hechos relacionados con el problema para abordar con mayor precisión el problema, la historia con sus deficiencias y el estado actual, este enfoque para permitirnos llevar a cabo la recopilación de información y datos de investigación.

Diseño de investigación

El objetivo de la investigación está basado en Evaluar las vulnerabilidades o riesgos en el sistema de información de la ferretería FERREQUIM, desarrollándose en el diseño de investigación no experimental, teniendo en claro que esta investigación cuenta con el sustento adecuado de información.

Siendo un documento con la investigación exploratoria, para poder obtener las vulnerabilidades de la empresa, es el responsable del primer acercamiento para que en el futuro se puedan realizar estudios más detallados.

Además, se implementó la metodología de investigación cualitativa para interpretar el análisis de los datos recolectados, y para realizar el diagnóstico de la problemática se usó las técnicas de observación del lugar y la entrevista a los empleados de la empresa, para conocer el funcionamiento del lugar y como realizan los procesos, entre otros datos relevantes para la

investigación lo cual permitió detectar las vulnerabilidades en los sistemas de información de la empresa FERREQUIM SA".

Pregunta 1.

- ¿Usted está consciente de las vulnerabilidades o riesgos que puede sufrir los sistemas de información en la ferretería FERREQUIM S.A. en 2022?

Pregunta 2.

- ¿Reciben ustedes capacitación para el correcto uso o manejo de los sistemas de información dentro de la ferretería FERREQUIM S.A. en 2022?

Pregunta 3.

- ¿Usted cree estar capacitado para el correcto uso y manejo del hardware y software de los sistemas de información dentro de la ferretería FERREQUIM S.A. en 2022?

Pregunta 4.

- ¿Cuentan con personal encargado del mantenimiento para el hardware y software de los sistemas de información dentro de la ferretería FERREQUIM S.A. en 2022?

Pregunta 5.

- ¿Con que frecuencias se realizan testeos de seguridad y auditorías internas en la ferretería FERREQUIM S.A.?

Pregunta 6.

- ¿Conoce usted las normas de seguridad de la información que se implementa dentro de la ferretería FERREQUIM S.A. en 2022?

Pregunta 7.

- ¿Cree que las normas y protocolos establecidos aseguran la integridad de la información de la ferretería FERREQUIM S.A. en 2022?

Pregunta 8.

- En su experiencia dentro de la empresa ¿Se han reportado casos de pérdidas de información o fallos en los procesos que realizan en la ferretería FERREQUIM S.A.?

Pregunta 9.

- ¿Como es la conectividad en la ferretería FERREQUIM S.A.?

La matriz de a continuación, muestra las debilidades que elevan el grado de riesgo a la vulnerabilidad en el sistema de información para el soporte de inventario de la ferretería FERREQUIM S.A. Los puntos de riesgos mostrados en la imagen de matriz, nos da a entender que todos los resultados son importantes, pero hay que poner más importancia a los problemas Altos de color rojo, y Medios de color amarillos

N°	Identificación de riesgo		Análisis del riesgo							
	Escenario de riesgo	Riesgo	Probabilidad			Impacto			Resultados	Categoría
			A (3)	M (2)	B (1)	A (3)	M (2)	B (1)		
1	Software	Falta de actualización de software (proceso y recursos)								
		Código troyano								
		Virus								
		Falla de software / corrupción								

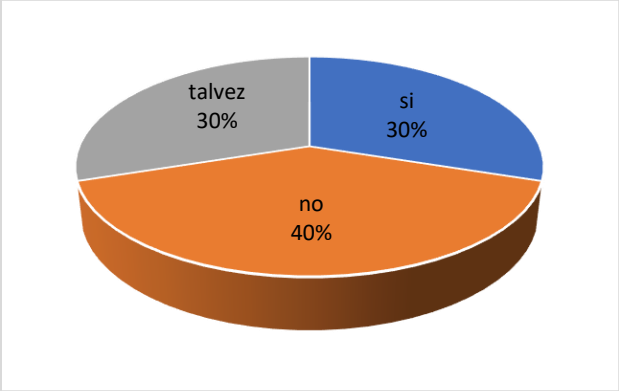
2	**Red**	Red inalámbrica expuesta al acceso no autorizado								
		Acceso electrónico no autorizado a sistemas externos								
		Acceso electrónico no autorizado a sistemas internos								
3	**Hardware**	Infección de sistemas a través de Unidades portables sin escaneo								
		Exposición o extravío de equipo, Unidades de almacenamiento, etc.								
		Perdida de datos por error hardware								
		Falta de mantenimiento físico (proceso, repuestos e insumos)								
4	**Datos**	Manejo inadecuado de datos críticos (codificar, borrar, etc.)								
		Transmisión no cifrada de datos críticos								

RESULTADOS

Pregunta 1.

- ¿Usted está consciente de las vulnerabilidades o riesgos que puede sufrir los sistemas de información en la ferretería FERREQUIM S.A. en 2022?

Gráfico 1

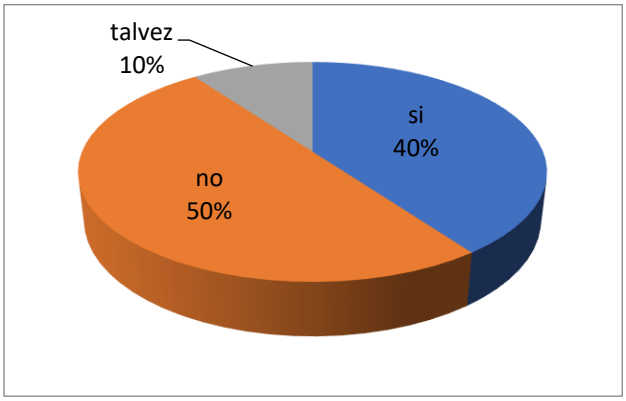


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 2.

- ¿Reciben ustedes capacitación para el correcto uso o manejo de los sistemas de información dentro de la ferretería FERREQUIM S.A. en 2022?

Gráfico 2

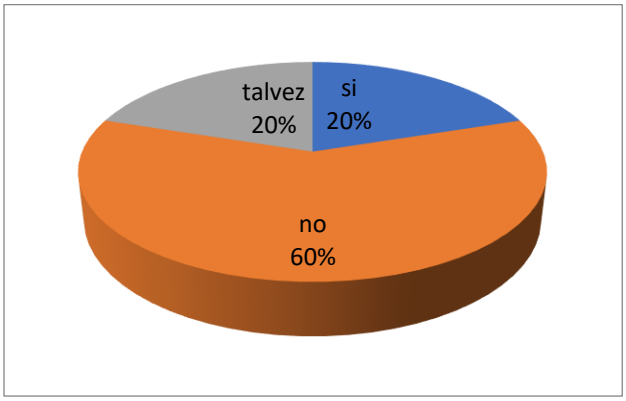


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 3.

- ¿Usted cree estar capacitado para el correcto uso y manejo del hardware y software de los sistemas de información dentro de la ferretería FERREQUIM S.A. en 2022?

Gráfico 3

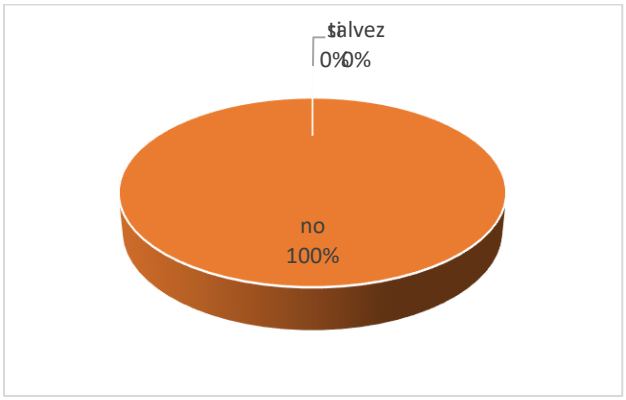


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 4.

- ¿Cuentan con personal encargado del mantenimiento para el hardware y software de los sistemas de información dentro de la ferretería FERREQUIM S.A. en 2022?

Gráfico 4

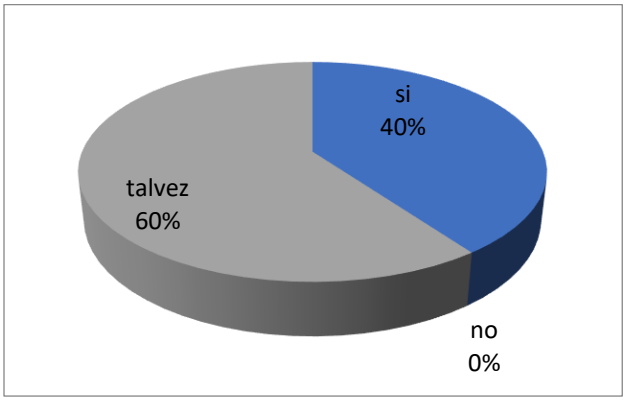


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 5.

- ¿Se realizan testeos de seguridad y auditorías internas en la ferretería FERREQUIM S.A.?

Gráfico 5

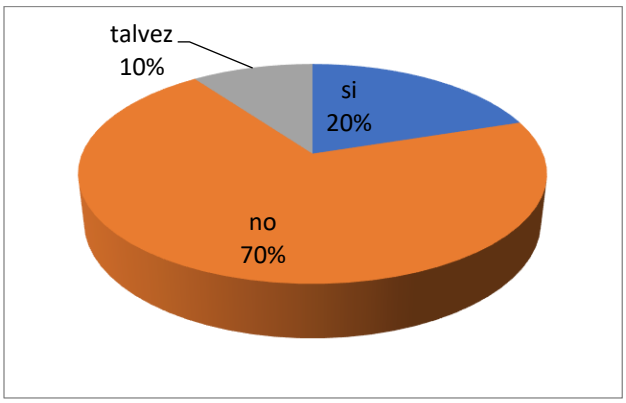


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 6.

- ¿Conoce usted las normas de seguridad de la información que se implementa dentro de la ferretería FERREQUIM S.A. en 2022?

Gráfico 6

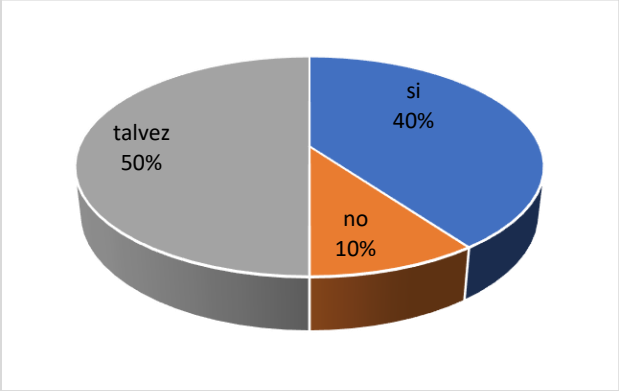


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 7.

- ¿Cree que las normas y protocolos establecidos aseguran la integridad de la información de la ferretería FERREQUIM S.A. en 2022?

Gráfico 7

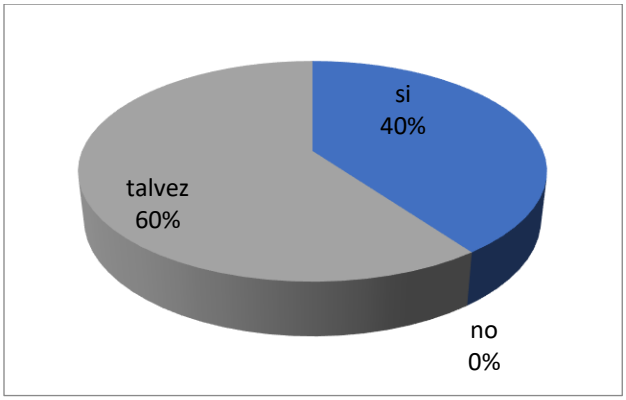


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 8.

- En su experiencia dentro de la empresa ¿Se han reportado casos de pérdidas de información o fallos en los procesos que realizan en la ferretería FERREQUIM S.A.?

Gráfico 8

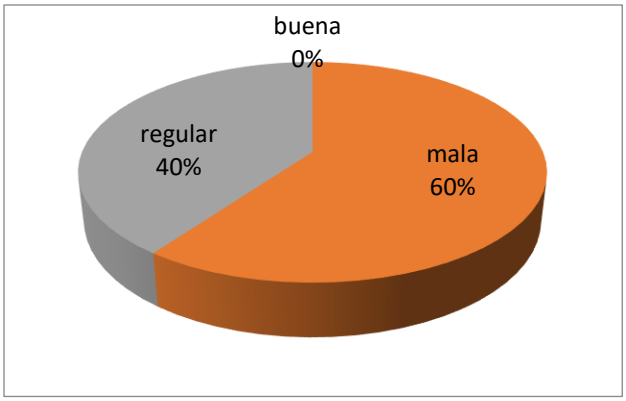


Elaborado por: Berruz Gordillo Jomira Katherine

Pregunta 9.

- ¿Como es la conectividad en la ferretería FERREQUIM S.A.?

Gráfico 9



Elaborado por: Berruz Gordillo Jomira Katherine

Tabla 2.

Análisis de Riesgo en los sistemas de información en la ferretería FERREQUIM S.A

N°	Identificación de riesgo		Análisis del riesgo							
	Escenario de riesgo	Riesgo	Probabilidad			Impacto			Resultados	Categoría
			A (3)	M (2)	B (1)	A (3)	M (2)	B (1)		
1	Software	Falta de actualización de software (proceso y recursos)	x					x	33%	AL
		Código troyano		x			x		44%	MM
		Virus		x				x	22%	ML
		Falla de software / corrupción	x				x		66%	AM
2	Red	Red inalámbrica expuesta al acceso no autorizado		x			x		44%	MM
		Acceso electrónico no autorizado a sistemas externos	x				x		66%	AM
		Acceso electrónico no autorizado a sistemas internos	x				x		66%	AM
3	Hardware	Infección de sistemas a través de Unidades portables sin escaneo		x			x		44%	MM
		Exposición o extravío de equipo, Unidades de almacenamiento, etc.	x			x			100%	AS
		Perdida de datos por error hardware		x		x			66%	MS
		Falta de mantenimiento físico (proceso, repuestos e insumos)		x			x		44%	MM
4	Datos	Manejo inadecuado de datos críticos (codificar, borrar, etc.)		x		x			66%	MS
		Transmisión no cifrada de datos críticos	x			x			100%	AS

Elaborado por: Berruz Gordillo Jomira Katherine

DISCUSIÓN DE RESULTADOS

La pregunta número uno muestra el conocimiento de los trabajadores sobre las vulnerabilidades o riesgos de los sistemas de información, donde el 40% de los encuestados no cuentan con el conocimiento de lo peligroso que son las vulnerabilidades, mientras que un 30% si y el otro 30% talvez.

En la pregunta numero dos se quiere conocer si los empleados cuentan con una correcta capacitación en el manejo de los sistemas informáticos en la ferretería, donde el 50% no cuenta con una capacitación, en cuanto a un 40% si saben manejar ciertos equipos.

También surgió la duda de saber quiénes ya estaban capacitados para un correcto uso de los hardware y software de la ferretería, pero solo un 20% contaba con conocimiento, y el 60% no sabían.

El mantenimiento es parte de los sistemas de información, pero los trabajadores aseguran con un 100% que la empresa no cuenta con un personal de mantenimiento al hardware y software.

La quinta pregunta busca saber si la empresa cuenta con un testeo de seguridad o si existen auditorías internas, pero el 60% están en duda con un talvez, y en 40% aseguran que si se hacen testeos de seguridad.

Se necesitaba saber si los empleados conocen algunas normas de seguridad de la información, las cuales se implementan dentro de la ferretería, pero el 70% no tienen conocimiento sobre las normas de seguridad de la información. Después se preguntó si los empleados creían que las normas y protocolos aseguraban a integridad de la información en la ferretería, y solo el 40% estaban seguro de ello, el 50% dudaban con un talvez.

Gracias a las preguntas anteriores, se pudo generar la pregunta número ocho, aquella que averiguaba sobre las pérdidas de información o si existieron fallos en los procesos sistemáticos de la empresa, donde el 60% se quedó en un talvez, dando a entender que ocurrieron fallos, pero se solucionaron, y el 40% están seguros que si existieron perdidas de información. Esto se pudo generar por los varios problemas que ya se mencionó antes, incluso el de la pregunta nueve, la cual buscaba en saber cómo era a conexión a internet de la empresa, estando en un 60% como mala, y el 40% regular.

La matriz de riesgo nos quiere demostrar la probabilidad y el impacto que ocasionan los escenarios de riesgos en la ferretería FERREQUIM S.A. El escenario del Software, demuestra que el 66% del análisis puede ocurrir por fallas de software o corrupción, siendo el resultado más alto. Los riesgos de la Red son más peligrosos, por la pérdida de información ocasionadas a través de accesos electrónicos externos no autorizados y los accesos electrónicos internos no autorizados.

El hardware no es fácil de infectar, pero la información que contiene es muy importante, y si esto se pierde o daña el riesgo es muy grande, un 100% es por errores de los mismos empleados, o el encargado de los dispositivos, este es por la pérdida de ciertos equipos de almacenamientos, y un 66% eliminación o perdida de datos por error del hardware. En cuanto a los Datos, el error más común pero el que tiene un impacto como una probabilidad alta, es la transmisión de datos no cifrados, los que son fáciles de obtener si no se protegen correctamente.

CONCLUSIONES

De las encuestas, se determinó que los empleados no son conscientes de las vulnerabilidades del sistema, incluso, no cuentan con capacitaciones para el correcto uso de los sistemas de información, esto perjudica a la empresa porque la información de todos los procesos no está asegurada ni presenta garantías de integridad. esto puede generar brechas de vulnerabilidades.

De la misma forma la empresa no sostiene un equipo de mantenimiento, y entre los trabajadores no existe alguien con conocimientos en el área informática para poder estar al tanto de las fallas del sistema, incluso, nadie esta seguro si la empresa cuenta con un equipo o con un periodo que haga seguimiento a la seguridad informática de la empresa.

Algunos empleados no están conscientes si la empresa sufre o ha sufrido de fallos como la perdida de información o errores en los procesos sistemáticos, pero otros empleados están seguros que varios de los documentos guardados en la nube o en las computadoras de la ferretería se han corrompido o eliminados.

Para finalizar, la matriz de riesgo, nos explica de manera mas detallada que el software de la empresa puede sufrir mas daño por parte de troyanos o fallas en el software. La red de la empresa es vulnerable, siendo expuesta al acceso no autorizado, externos o internos.

La vulnerabilidad de hardware significa la probabilidad de que una parte física del sistema falle debido a un mal uso, descuido, mal diseño, etc., dejando el sistema desprotegido o inoperable. También cubre las formas en que las personas pueden usar el hardware para atacar la seguridad del sistema, como sabotear el sistema al sobrecargarlo intencionalmente con componentes de hardware no diseñados adecuados para ejecutarse en el sistema.

Las vulnerabilidades de datos, describe que la transmisión de datos no cifradas contiene un impacto algo, y a la vez siendo algo muy común. En el envió de datos estos se pueden corromper, o llegar de manera distorsionada al destino siendo un riesgo alto para la compañía.

.

RECOMENDACIÓNES

Es recomendable que todos los empleados y administrativos de la empresa reciban capacitaciones sobre normas de seguridad de la información, seguridad básica de hardware y software como apoyo al proceso de asegurar la información.

Se recomienda hacer revisiones periódicas a los sistemas informáticos, como el hardware y software, entre ellos, la condición de los computadores, actualizaciones de drivers, la seguridad de los archivos encriptados y cambiar siempre la autentificación de dos pasos de la nube y sus contraseñas, con el fin de hacer un seguimiento en la empresa para detectar posibles vulnerabilidades y brindar soluciones a tiempo.

Para el hardware recomienda asegurarse que las unidades estén en un óptimo ambiente que permita aprovechar todas sus características y potencia para realizar los procesos más eficientes.

En los datos se recomienda utilizar algoritmos cifrada de datos para asegurar la integridad de la información y esta no se vea expuesta a terceros.

REFERENCIAS

Alano, D. (5 de septiembre de 2021). *isbel*. Obtenido de isbel: https://isbel.com/seguridad-de-la-informacion-vulnerabilidades-riesgos/

BERTOLIN, J. A. (2008). *Seguridad de la información. Redes informática y sistemas de información. .* España: Paraninfo.

Cardona, O. D. (s.f.). *desenredando*. Obtenido de desenredando: https://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

De Pablos Heredero, C., López Hermoso Agius, J. J., Martín-Romo Romero, S., & Medina Salgado, S. (2019). *Organización y transformación de los sistemas de información en la empresa.* Madrid: ESIC editorial. Obtenido de Dialnet.

Gomez, A. (2014). *Enciclopedia de la seguridad informatica.* España: RA-MA.

implementandosgi. (s.f.). *implementandosgi*. Obtenido de implementandosgi: https://www.implementandosgi.com/procesos/analisis-de-vulnerabilidad-plan-de-emergencias/

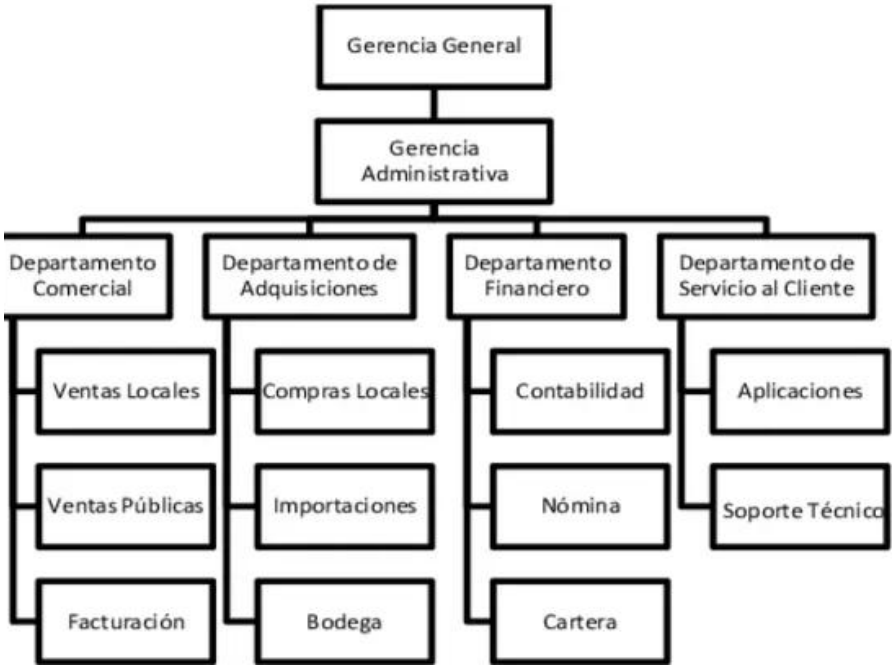
Lederkremer, M. (2019). *Redes informaticas.* Buenos aires: REdusers.

Romero, M. y. (2018). *introduccion a la seguridad informatica y el analisis de las vulnerabilidades.* Manabi: Editorial Area de innovacion y desarrollo 3ciencias.

Tarazona, C. (2007). Amenazas informaticas y seguridad de la informacion . *HeinOnline*, 137. Obtenido de HeinOnline: https://heinonline.org/HOL/LandingPage?handle=hein.journals/dpencrim28&div=29&id=&page=

ANEXO

Anexo 1: organigrama de la empresa



Anexo 2: entrevista

GUÍA DE OBSERVACIÓN

NOMBRE DE LA EMPRESA:	FERREQUIM SA
CASO DE ESTUDIO:	VULNERABILIDADES EN EL SISTEMA DE INFORMACION EN EL SOPORTE DE INVENTARIO DEL DISTRIBUIDOR MAYORISTA DE PRODUCTOS DE FERRETERIA ¨FERREQUIM SA¨
ESTUDIANTE:	Jomira Katherine Berruz Gordillo

OBJETIVO: Evaluar las vulnerabilidades o riesgos en el sistema de información de la ferretería ¨FERREQUIM SA¨ y posteriormente proponer una solución

MÉTODO: ENCUESTA

N.0	PREGUNTAS
1	**USTED ESTA CONSIENTE DE LAS VULNERABILIDADES O RIESGOS QUE PUEDEN SUFRIR LOS SISTEMAS DE INFORMACION EN LA EMPRESA FERREQUIM SA.** SI [ ] NO [ ] TALVEZ[]
2	**RECIBEN CAPACITACIONES PARA EL CORRECTO USO O MANEJO DE LOS SISTEMAS DE INFORMACION EN LA EMPRESA FERREQUIM SA .** SI [ ] NO [ ] TALVEZ[]
3	**CUENTA CON EL PERSONAL ENCARGADO DEL MANTENIMIENTO PARA EL HARDWARE Y SOFTWARE EN LA EMPRESA FERREQUIM SA.** SI [ ] NO [ ] TALVEZ[]
4	**USTED CREE ESTAR CAPACITADO PARA EL CORRECTO USO Y MANEJO DEL SOFTWARE Y HARDWARE DE LOS SISTEMAS DE INFORMACION EN LA EMPRESA FERREQUIM SA.** SI [ ] NO [ ] TALVEZ[]
5	**¿CONOCE USTED LAS NORMAS DE SEGURIDAD DE LA INFORMACIÓN QUE SE IMPLEMENTAN EN LA EMPRESA?** SI [ ] NO [ ] TALVEZ[]
6	**¿**SE **REALIZAN TESTEOS DE SEGURIDAD Y AUDITORÍAS INTERNAS EN LA EMPRESA?** SI [ ] NO [ ] TALVEZ[]
7	**CREE QUE LAS NORMAS Y PROTOCOLOS ESTABLECIDOS ASEGURAN LA INTEGRIDAD DE LA INFORMACIÓN DE LA EMPRESA.** SI [ ] NO [ ] TALVEZ[]

8	**EN SU EXPERIENCIA EN LA EMPRESA ¿SE HAN REPORTADO CASOS DE PERDIDA DE INFORMACIÓN O FALLO EN LOS PROCESOS QUE REALIZAN EN LA EMPRESA?** SI [ ] NO [ ] TALVEZ[]
9	**¿COMO ES LA CONECTIVIDAD EN LA FERRETERÍA FERREQUIM S.A.?** BUENA [ ] MALA [ ] REGULAR[]

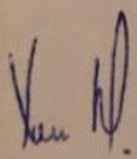
Babahoyo, 16 de marzo del 2022

Sr.
Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO DE LA FACULTAD DE ADMINISTRACION, FINANZAS E INFORMATICA

En su despacho. –
Reciba un cordial saludo de parte del **ING. XAVIER DELGADO QUINTANA,** representante legal de la empresa **FERREQUIM S.A,** el motivo de la presente es para informarle que se le fue otorgado el permiso correspondiente para realizar su caso de estudio con el tema **VULNERABILIDADES EN EL SISTEMA DE INFORMACION EN EL SOPORTE DE INVENTARIO DEL DISTRIBUIDOR MAYORISTA DE PRODUCTOS DE FERRETERIA DE LA EMPRESA FERREQUIM SA DE LA CIUDAD DE GUAYAQUIL** a la señorita **JOMIRA KATHERINE BERRUZ GORDILLO** con cédula de identidad NO. **1207155159,** estudiante de la carrera de Ingeniería en Sistemas de Información, matriculada en el proceso de titulación en el periodo noviembre 2021- abril 2022 para la obtención de su grado académico profesional universitario de tercer nivel como **INGENIERA EN SISTEMAS DE INFORMACION.**

Siendo su petición aceptada me despido amablemente.

Atentamente:



Ing. Xavier Delgado Quintana
Representante de la empresa FERREQUIM S.A