UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA "FERRETERÍA ARMIJOS" DE LA CIUDAD DE MACHALA.

RAMON PLACENCIO LIDIA AMARILIS
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA "FERRETERÍA ARMIJOS" DE LA CIUDAD DE MACHALA.

RAMON PLACENCIO LIDIA AMARILIS
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2020

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORIA DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA "FERRETERÍA ARMIJOS" DE LA CIUDAD DE MACHALA.

RAMON PLACENCIO LIDIA AMARILIS
INGENIERA EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 21 DE FEBRERO DE 2020

MACHALA
21 de febrero de 2020

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado AUDITORIA DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA "FERRETERÍA ARMIJOS" DE LA CIUDAD DE MACHALA., hacemos constar que luego de haber revisado el manuscrito del precitado trabajo, consideramos que reúne las condiciones académicas para continuar con la fase de evaluación correspondiente.

GONZALEZ SANCHEZ JORGE LUIS
0703333898
TUTOR - ESPECIALISTA 1

PARRA OCHOA EUDORO BENITO
0701063406
ESPECIALISTA 2

OCHOA CAICEDO HECKLER ROTHWELL
0702681917
ESPECIALISTA 3

AUDITORIA DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA “FERRETERÍA ARMIJOS” DE LA CIUDAD DE MACHALA

por Lidia Amarillis Ramón Placencio

Fecha de entrega: 09-feb-2020 11:41a.m. (UTC-0500)
Identificador de la entrega: 1253981068
Nombre del archivo: RAMON_PLACENCIO_LIDIA_AMARILIS.pdf (537.4K)
Total de palabras: 3682
Total de caracteres: 20687

CLÁUSULA DE CESIÓN DE DERECHO DE PUBLICACIÓN EN EL REPOSITORIO DIGITAL INSTITUCIONAL

La que suscribe, RAMON PLACENCIO LIDIA AMARILIS, en calidad de autora del siguiente trabajo escrito titulado AUDITORIA DE LA SEGURIDAD INFORMÁTICA DE LA EMPRESA "FERRETERÍA ARMIJOS" DE LA CIUDAD DE MACHALA., otorga a la Universidad Técnica de Machala, de forma gratuita y no exclusiva, los derechos de reproducción, distribución y comunicación pública de la obra, que constituye un trabajo de autoría propia, sobre la cual tiene potestad para otorgar los derechos contenidos en esta licencia.

La autora declara que el contenido que se publicará es de carácter académico y se enmarca en las dispociones definidas por la Universidad Técnica de Machala.

Se autoriza a transformar la obra, únicamente cuando sea necesario, y a realizar las adaptaciones pertinentes para permitir su preservación, distribución y publicación en el Repositorio Digital Institucional de la Universidad Técnica de Machala.

La autora como garante de la autoría de la obra y en relación a la misma, declara que la universidad se encuentra libre de todo tipo de responsabilidad sobre el contenido de la obra y que asume la responsabilidad frente a cualquier reclamo o demanda por parte de terceros de manera exclusiva.

Aceptando esta licencia, se cede a la Universidad Técnica de Machala el derecho exclusivo de archivar, reproducir, convertir, comunicar y/o distribuir la obra mundialmente en formato electrónico y digital a través de su Repositorio Digital Institucional, siempre y cuando no se lo haga para obtener beneficio económico.

Machala, 21 de febrero de 2020

RAMON PLACENCIO LIDIA AMARILIS
0703132340

RESUMEN

La innovación tecnológica es una herramienta importante para el desarrollo de una empresa; hoy en día es muy fácil manejar el aspecto logístico de una empresa, los datos y archivos importantes pueden guardarse de manera digital dentro de ordenadores de los cuales se puede acceder desde cualquier sitio en caso de tener internet; además, se pueden llevar registro de inventario y demás actividades realizadas por la entidad, se puede optimizar el trabajo disminuyendo el tiempo en que se lo ejecuta y aumentando su rendimiento. Todo esto gracias a las innovaciones de la tecnología. Dentro de cada entidad existe un departamento encargado de manejar y controlar que exista confidencialidad de estos datos para la empresa, este verifica que no haya intrusos queriendo acceder a esa información privada; en el mercado hay muchas herramientas que sirven para llevar un adecuado control de la seguridad informática. En este documento se pretende establecer que tan buena es la seguridad informática en la empresa "Ferretería Armijos" a través de una auditoria informática. Para llevar a cabo esto, se indaga en varias bases de datos de donde se extraen artículos de revistas científicas, calificados para ser citados en un proyecto investigativo; esta información debe tener contenido relevante para que aporte significativamente a la investigación.

PALABRAS CLAVE: Auditoría informática, empresas, ferretería, seguridad informática, riesgos informáticos.

ABSTRACT

Technological innovation is an important tool for the development of a company; Nowadays it is very easy to manage the logistic aspect of a company, important data and files can be stored digitally in computers which can be accessed from any site in case you have internet; In addition, the registration of inventory and other activities carried out by the entity can be carried out, the work can be improved by reducing the time it was executed and increasing its performance. All this thanks to the innovations of technology. Within each entity there is a department responsible for managing and controlling the confidentiality of this data for the company, this verifies that there are no intruders who open access to that private information; In the market there are many tools that serve to carry out an adequate control of computer security. This document is intended to establish how good is computer security in the company "Ferretería Armijos" through a computer audit. To carry out this, it is investigated in several databases from which articles are extracted from scientific journals, qualified to be cited in a research project; This information must have relevant content so that it contributes relevant to the investigation.

KEYWORDS: IT audit, companies, hardware store, computer security, computer risks.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE CUADROS

1. INTRODUCCIÓN

El origen de las empresas en el mundo se remonta a muchos años atrás, estas con el paso del tiempo han ido acrecentándose a medida que se desarrolla la sociedad, pero no fue solo hasta que la Revolución Industrial ocurrió que se dio el verdadero desarrollo de la industria.

Hoy en día se puede observar que existen muchas empresas que se dedican a la producción y comercialización de sus productos, para lo cual utilizan distintos medios entre ellos los digitales mediante los cuales pueden atraer más clientes y lograr ventas seguras. Los medios digitales también son utilizados para guardar información perteneciente a la empresa, misma que una vez digitalizada puede ser abordada desde cualquier sitio, lo cual representa un enorme peligro debido a la cantidad de personas ajenas a la institución que pretenden acceder sin permiso a dicha información.

La seguridad informática tiene gran importancia pues debido al contenido que alberga se puede decir que de esta depende el fututo de la empresa.

Existen varias herramientas que se utilizan para guardar esta información y evitar percances con cyber atacantes, sin duda son útiles, pero es necesario saber que tanto para poder elegirlas de entre otras. En las empresas hay un departamento encargado del manejo informático en donde se requiere personal capacitado para resolver los problemas informáticos que se presenten.

Muchas veces se tiene la inconciencia de colocar personas que no tienen la suficiente capacidad para ejercer tales actividades, generando percances por el mal manejo de los equipos o aplicaciones.

En vista del conocimiento de estos problemas es necesario realizar una auditoría informática que contemple la revisión de todos estos aspectos mediante la cual se pueda encontrar la forma de optimizar los recursos disponibles en la empresa, establecer políticas que cumplan con el correcto manejo y mantenimiento tanto de equipos como de programas, analizar el uso de las herramientas disponibles y verificar que se cumplan con lo establecido previamente por la empresa, además de estudiar las redes informáticas disponibles dentro de la entidad y comprobar que cumplan con los requerimientos de la empresa.

La formulación del problema es ¿Cómo analizar la seguridad informática de la Ferreteria Armijos? Es una realidad que las cualidades digitales potencian los negocios, pero pocos empresarios están al tanto de sus adversidades e integran medidas de seguridad para cuidar sus activos lógicos.

El objetivo es analizar la seguridad computacional de la empresa "Ferretería Armijos" de la ciudad de Machala, mediante una auditoria informática para identificar vulnerabilidades y proponer controles respectivos.

Se aplica una metodología de carácter explorativo, recopilando conceptos y datos de campo al ser procesados mediante un análisis deductivo e inducir cuales controles son los oportunos en base a las debilidades diagnosticadas.

Finalmente se presentan conclusiones de la investigación realizada, en donde constan los puntos de vista y consideraciones finales obtenidas con la realización de este estudio.

2. DESARROLLO:

2.1 Marco Teórico

A continuación, se explica teóricamente las conceptualizaciones relacionadas al objeto de estudio. Utilizando la investigación bibliográfica se ha podido encontrar conceptos clave para el aprendizaje y entendimiento de la temática planteada, en este caso se abordan temas que guardan relación con la auditoria informática; estos se describen a continuación:

2.1.1 Auditoría informática.

Una auditoría corresponde a un proceso que evalúa los procesos llevados a cabo en la institución e identifica irregularidades producidas en torno a la gestión de estos procesos, examina el cumplimiento de los objetivos y garantiza que se cumplan aquellos que aún se encuentran pendientes otorgando la seguridad necesaria del cumplimiento en base a las normativas y legislaciones de la entidad (Cantos, 2019).

Entonces se puede decir que a medida que el mundo avanza, aparecen nuevas empresas en el mundo que originan actividades complejas para su desarrollo, lo cual hace necesario que se requiera de personal completamente capacitado para ejecutar dichos trabajos de manera eficiente, sin embargo, suelen aparecer situaciones en donde la falta de capacitación de los empleados genera negligencia en la ejecución de los procesos y en el uso de los recursos, dando resultados negativos a la empresa. La auditoría surge como una necesidad de controlar que se cumplan los procedimientos de la manera más idónea (Hernández, 2016).

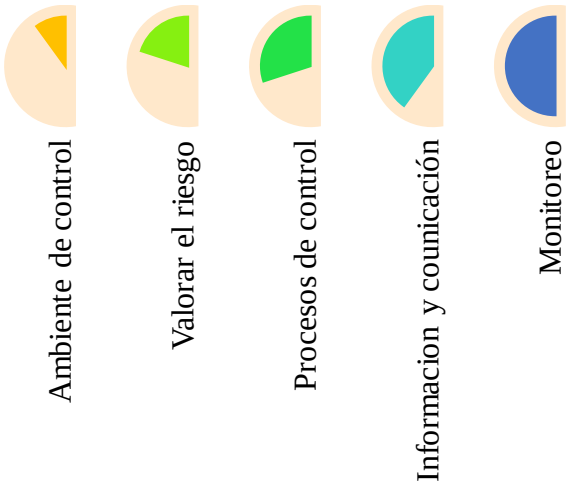

Ilustración 1. Componentes del control interno en una empresa.

Fuente: *(Hernández, 2016)*

En particular, las empresas a medida que pasa el tiempo se vuelven más dependientes de la tecnología con la que administran sus recursos y los ponen a disposición del público, en ese aspecto se dice que el éxito de la empresa depende entre otras cosas de los recursos tecnológicos que posee. Arcentales y Caycedo (2017) indican la importancia de la aplicación de una auditoría que evalúe periódicamente los procesos para comprobar su calidad y capacidad de acuerdo a lo requerido por la empresa. Además, que a medida que se incrementa el número de empresas en el mundo, crece también el volumen de información que debe ser manejada, para ello se ha tomado la decisión de automatizar los procesos y digitalizar los datos.

Este recurso tecnológico es uno de los más importantes dentro de la empresa por lo cual se requiere que se le examine para verificar su calidad y seguridad que brinda al manejar la información; esto se lleva a cabo mediante la auditoria informática.

La seguridad de la información se vuelve una tarea importante pues se maneja datos de interés meramente internos, por ello es indispensable resguardarla a fin de evitar riesgos y daños por parte de ajenos a la institución.

Una auditoria informática permite detectar falencias en el manejo de los sistemas de información, así como también ayudan al ajuste de la plataforma informática, verifica el estado de los contratos con la empresa que suministra los bienes o servicios digitales y evalúa la calidad del servicio prestado en relación a las tecnologías de información y comunicación (Arcentales & Caycedo, 2017).

2.1.2 Seguridad informática.

La seguridad informática está dirigida a la protección de la información, recursos contables, contexto legal y otros bienes perceptibles e imperceptibles de la institución.

Esta disciplina aplicada al sistema informático como a cualquier otro, pretende reducir o disolver los peligros informáticos a los que se expone la información cuyos causantes son las personas externas a la institución que valiéndose de falsas identidades o accesos no permitidos intentan acceder a los datos de la empresa con fines perversos. “El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como información, hardware o software” (Gil y Gil, 2017, p.194). En este aspecto se señala que la seguridad informática se dirige al cuidado de la integridad del recurso tecnológico que posee la empresa, albergando a los equipos computacionales y a la información digitalizada.

La aparición de las nuevas tecnologías de información y comunicación han ampliado los horizontes de las organizaciones sirviendo como puente entre estas y el éxito; el mal manejo, la pérdida o la difusión de esta puede provocar incalculables pérdidas, ocasionar problemas legales e incluso puede representar el fracaso para la empresa.

La falla en la seguridad informática puede ser causa de diferentes factores, estos se describen a continuación:

Cuadro 1. Factores que generalmente son los causantes de la falla en la seguridad informática.

Causantes de fallas en la seguridad informática	
Hackers	Invaden la red y acceden a los servidores para sustraer información
Virus informáticos	Infectan y dañan los programas utilizados por la empresa
Espías industriales	Acceden a los servidores con el fin de averiguar los planes de la empresa
Empleados de la empresa	En ocasiones, los espías pueden ser los mismos empleados que acceden a información privada para divulgarla ante una organización contraria.

Fuente: Elaboración propia

Se puede destacar que la seguridad informática es aplicada con el fin de mantener lejos cualquier peligro que atente contra el buen estado de la información, para ello existen 2 objetivos principales, el primero es la disminución de riesgos informáticos latentes en el medio, permitiendo continuar con normalidad los procesos de la empresa, sin generar gastos extra; el segundo es dar garantía de confidencialidad a los archivos y documentos de la organización (Quiroz y Macías, 2017).

Es decir, con la seguridad informática se pretende cuidar y mantener a buen recaudo todo el recurso tecnológico de la organización, en ello interviene un personal capacitado que ejecute cada proceso de manera responsable.

Actualmente la seguridad informática dotada de los mejores recursos es aquella que mayor demanda tiene por las empresas y distintas organizaciones en el mundo; en caso de darse una mala gestión o una planificación deficiente podrían ocasionarse complicaciones en el desarrollo de la empresa además de adquirir problemas en la seguridad informática.

El inmensurable crecimiento económico y desarrollo de la sociedad provocan cambios a los que el ser humano sin duda debe adaptarse; como resultado a este desmedido desarrollo el hombre queda vulnerable y susceptible a lo que venga creando así una

dependencia a muchas cosas entre ellas a la tecnología, pues con el uso de esta el ser humano es capaz de realizar muchos procesos que manualmente le serían muy complicados.

Las empresas que han integrado las nuevas TIC en su funcionamiento organizacional poseen ciertas características que hacen necesario tomar un cambio en la aplicación de auditorías informáticas (Díaz, Pérez, & Proenza, 2014).

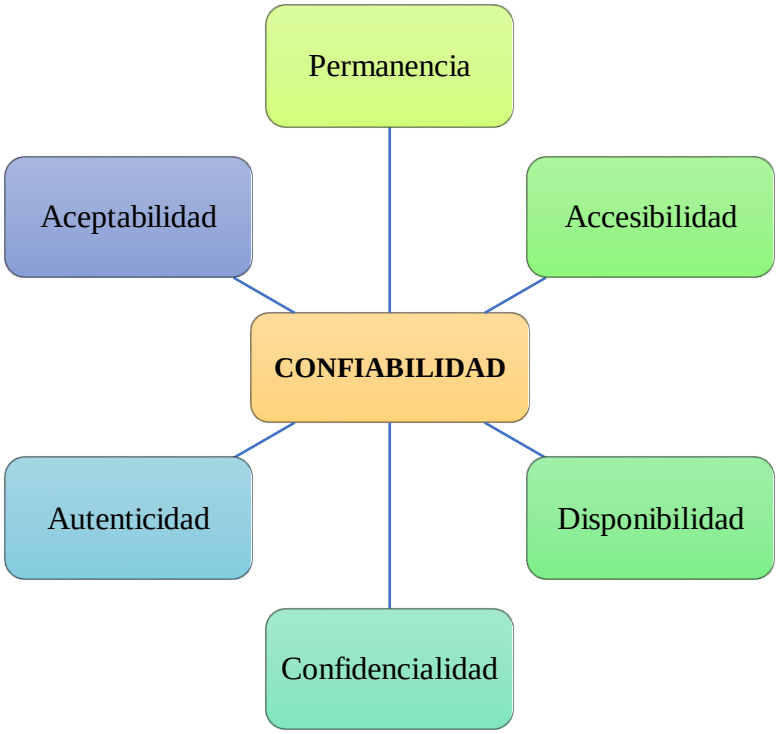

Ilustración 2. Características de la confiabilidad (seguridad informática).

Fuente: (Quiroz & Macías, 2017)

2.1.3 Herramientas utilizadas en Auditorías informáticas.

La auditoría informática es un procedimiento ejecutado por verdaderos profesionales capacitados para ello; en este proceso se recolecta, reúne y analiza la información encontrada para establecer si se cumplen con normalidad las funciones del departamento informático; funciones como: proteger los bienes empresariales, conservar la confidencialidad de los datos internos, uso adecuado de los recursos y cumplimiento de los procesos de acuerdo a los reglamentos establecidos. Una auditoría informática es un proceso realizado a manera de control para identificar amenazas o riesgos a los que podría estar expuesto el sistema informático de una organización, este proceso varía dependiendo las condiciones y necesidades de la entidad ejecutora, pues el recurso económico es clave para determinar el tipo de auditoria a realizarse.

Este proceso auditor es llevado a cabo con el uso de algunas herramientas que concretan las distintas técnicas escogidas para la auditoria informática. Entre las herramientas más comúnmente utilizadas están las siguientes:

Entrevistas: Es una herramienta útil que se aplica a todo el personal que labora en el departamento informático, con la que se busca informarse acerca de las condiciones del departamento.

Una entrevista es utilizada como un instrumento recolector de datos con el fin de juntar la información necesaria para evaluar el objeto de estudio, además es un medio por el cual el entrevistador interactúa de manera verbal con el entrevistado, lo cual genera en el investigador la sensación conocer de mejor manera la posición del entrevistado por haberse relacionado con el objeto de estudio (Troncoso & Amaya, 2017).

Cuestionarios: para aplicar esta herramienta de recolección de datos es necesario identificar al objeto de estudio y la magnitud que representa en la investigación; sirve para tomar los distintos puntos de vista de los evaluados y finalmente tener una idea clara de la situación que atraviesa el objeto de estudio (Escofet, Folgueiras, Luna, & Palou, 2016).

Checklist: en la auditoría informática son utilizados para verificar el cumplimiento de una o varias actividades repetitivas programadas por la empresa, además ayuda a recolectar datos de manera ordenada y metódica.

Software de interrogación: hoy en día los softwares orientados a las auditorias informáticas están diseñados utilizando lenguajes de programación con los cuales se pueda interrogar las bases de datos de la empresa en auditoria.

Herramientas virtuales: estos son programas o aplicaciones virtuales con las cuales se puede auditar una empresa de una manera correcta, algunas de las principales herramientas virtuales se describen a continuación:

- COBIT: Esta es una metodología que se encarga de llevar el control de la información y detectar riesgos en los sistemas informáticos, desarrollando control sobre las tecnologías de la información actualizadas (Caiza & Bolaños, 2014).
- ITAF: Infromation Technology Assurance Framework (Marco de Aseguramiento de la Información Tecnológica), es una herramienta aplicable a cualquier tipo de

auditoria que actúa como evaluador de la capacidad del profesional auditor. Supervisa estándares generales como la evaluación de la forma en que se realizan los procesos internos en la institución respondiendo a la ética profesional, además verifica la planificación etc.

- NMAP: se emplea para explorar la red y encontrar información respecto a sistemas operativos y los riegos a los que se enfrenta, utiliza técnicas de escaneo para detectar intrusos en el sistema.

2.1.4 Riesgos y vulnerabilidades en el sistema informático de una empresa.

Actualmente se vive el boom tecnológico alrededor del mundo, el manejo de la información se ha facilitado debido al conjunto de herramientas disponibles en el medio, con ello han surgido nuevos riegos y vulnerabilidades a los que se expone la información en conjunto con los sistemas informáticos (Hernández & Mejia, 2015). Estos pueden representar gran peligro dependiendo del tipo que sean, los ataques más comunes suelen ser: la inyección SQL, ejecución de acciones en sitios cruzados, uso de información privada en sitios cruzados, etc.

Para detectar estos ataques y vulnerabilidades se suelen utilizar herramientas dedicadas a este fin con las que se puede analizar el riesgo que corre el sistema operativo, estas pueden ser de carácter estático o dinámico.

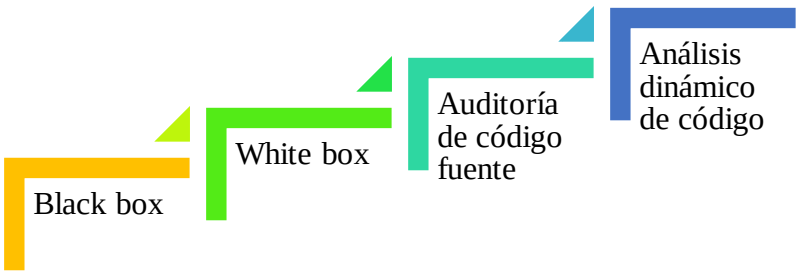

Ilustración 3. Técnicas utilizadas para detectar vulnerabilidades informáticas.

Fuente: (Hernández & Mejia, 2015)

Con una adecuada gestión de riesgos informáticos se puede detectar a tiempo cualquier amenaza latente, para manejarla, minimizarla y en el mejor de los casos combatirlas hasta que desaparezca; algo que beneficiará la situación de la organización, su sistema informático y sus clientes (Corda, Viñas, & Coria, 2017).

Con la prevención a tiempo de los riesgos y vulnerabilidades al sistema operativo, se puede evitar daños en la ejecución de proyectos, retrasos en la producción, plagio de información, etc.

2.1.5 Manejo de problemas informáticos.

Ante el desarrollo de la tecnología a nivel mundial, muchas empresas han optado por insertar las Tecnologías de Información al funcionamiento de la organización; con esto se espera contribuir a un mejor desempeño a nivel institucional y competitivo brindando los mejore servicios a los clientes.

López & Vázquez (2016), relatan que con el uso de estas tecnologías es posible competir en el mercado de manera eficaz pudiendo además organizar toda la información de la empresa de manera virtual posibilitando su acceso desde cualquier lugar.

Esta digitalización de datos incrementa el reto de mantenerla en custodia pues en el medio existen muchos peligros que atentan contra la seguridad de la información, esto vuelve necesario que se realice una adecuada gestión de riesgos que incluya una serie de técnicas que empleen las herramientas adecuadas para cumplir con el correcto cuidado de la información. Estos problemas informáticos al originarse desde distintos sitios y medio representan diversos tipos de complejidad por lo que su solución difiere un poco en los medios a utilizarse para ello, los problemas informáticos pueden ser tanto de carácter técnico como organizacionales (Solana, 2014), en el cuadro presentado a continuación se detalla su estructura:

Cuadro 2. Problemas informáticos de carácter organizacional.

PROBLEMAS DEL SISTEMA INFORMÁTICO	
Compromiso administrativo	Es un verdadero problema si la organización misma no le presta atención a los riesgos que atraviesa.
Seguridad	Los sistemas informáticos son más vulnerables desde que la tecnología empezó a tomar fuerza, y existe alta posibilidad de ataques externos.
Gestión de conocimiento	Los SI deben ser usados para guardar el conocimiento de la entidad, considerando ciertas medidas de seguridad.

Fuente: (Solana, 2014)

2.2 Caso Práctico

Comprende la resolución del problema, consiste en auditar a la empresa Ferretería Armijos para determinar sus vulnerabilidades informáticas, con el propósito de recomendar medidas de seguridad que mejoren su desempeño y gestión de TIC`s.

2.2.1 Ferretería "FERREARMIJOS".

Ilustración 4. Logo de la empresa Ferrearmijos.

Fuente: (CompuTrabajo, s.f.)

La empresa considerada para este proyecto es la Ferretería Armijos o Ferrearmijos S.A. cuya sede está ubicada en la ciudad de Machala (Ecuador). Es una empresa dedicada a la comercialización de materiales de construcción al por mayor y menor.

Esta empresa se fundó el 15 de agosto del año 2013, hasta el año 2018 contaba con apenas 60 empleados que eran los encargados de mantener funcionando la ferretería.

Según datos mostrados por la misma empresa, en el año 2018 se reportó incremento en los ingresos por concepto de ventas de productos, esto ascendió a un 14%, incrementando su capital actual en un 30% aproximadamente. El margen neto aumentó un 2,77% aproximadamente en el año 2018 (EMIS, 2020).

El local matriz de esta ferretería se ubica en la Av. La Ferroviaria & Mary Villavicencio, cuenta con 3 sucursales:

Sucursal 1: Cdla. Roldos Diescisiteava Sur Oeste y Quinta Este, Sucursal 2: Vía. Pto. Bolívar Treintadosava Oeste y Av. Bolívar Madero, y la Sucursal 3: 10 de Agosto y 8ava Norte.

Ilustración 5. Ubicación de Ferrearmijos.

Fuente: Google Maps

2.2.2 TIC's utilizadas en la empresa

La ferretería como toda entidad franquiciada, lleva contabilidad teniendo un sistema de facturación e inventario, opera con software comerciales y paquetes de software en base de datos que caracteriza a firmas como EDESA o DISENSA, para tener un control amplio de los precios, proveedores, ventas e implementar un monitoreo constante.

Cuadro 3. Tecnologías informáticas utilizadas en la empresa

NOMBRE	DESCRIPCIÒN	UTILIDAD
Sistema operativo Windows 10	Usan ordenadores para almacenar, tratar e interpretar informaciòn referente a su negocio.	Solventa los software, bases de datos, gesta uso de internet y redes locales al enviar datos.
Sistema de facturación e inventario	Es un software hecho por encargo en licencia libre, es dinámico y permite facturar, ajustar inventarios y llamar a proveedores.	Permite entregar facturas, analizar ventas, enviar pedidos en tiempo real y registrar contabilidad acorde a las normas vigentes.
Paquetería Office	Conjunto de programas, como Microsoft Word, Excel, Publisher, entre otras herramientas ofimáticas.	Procesar texto, llevar contabilidad en hojas de datos, analizar ventas, realizar banner u otras acciones en ordenador
Sistema de cámaras de vigilancia	Vigila tanto al personal como clientela, quien sale e ingresa a bodega y camiones de carga.	Permite controlar el desempeño laboral, cuidar los activos y tomar acciones en caso de robo.
Redes sociales y comunicación instantánea	Interactuar con la comunidad, darse a conocer y registrar demanda del mercado	Publicitar la empresa, mantener una comunicación con los clientes y ofertar promociones.

Fuente: Elaboraciòn Propia

Se aprecia que las TIC`s son esenciales en toda empresa, sin importar su tamaño o actividad.

2.2.3 Vulnerabilidades y debilidades detectadas

Como es propio de los sistemas digitales son susceptibles a fallos, hackeos e irregularidades que demandan tomar medias tanto preventivas como correctivas para mantener un desempeño optimo en la empresa.

Es indispensable mantener en buen estado las instalaciones eléctricas, redes e internet al conectarse con los sistemas que permiten su funcionamiento.

Las debilidades diagnosticadas en la entrevista y visita son:

- Fallos repentinos de energía eléctrica
- Hackeos o espionaje corporativo
- Pérdida o corrupción de datos e informaciòn
- Fallas en el sistema de facturación y bases de datos
- Cortes o interrupciones en el servicio de internet
- Errores en el sistema contable virtual
- Manipulaciones malintencionadas de las tecnologías
- No se aplica una metodología normada ni se realizan auditorías externas

2.2.3 Medidas de seguridad actuales

Entorno a la seguridad informática y desempeño de la ferretería, la gerencia imparte los controles detallados en el *cuadro 4.*

Cuadro 4. Medidas y controles aplicados en la empresa Ferri Armijos

COMPONENTE EMPRESARIAL	Estado
Sistema Eléctrico	Se tiene reguladores de voltaje y protecciones, por fallos constantes en la red, pero no se descarta cortes repentinos.
Redes e internet	Se alquila a empresas locales, cuenta con router, servidor propio, respaldos en la nube y técnicos capacitados.
Bases de datos en sistema de facturación	Cortafuegos, monitoreo de red, software de análisis y soporte en línea
Hardware y computadores	Antivirus, mantenimiento preventivo, predictivo y correctivo en forma semestral, se actualizan cada 3 años
Redes sociales	La imagen empresarial cuenta con un agente de marketing y un control riguroso de su informaciòn
Personal y talento humano	Cámaras de seguridad, sistemas biométricos y reuniones regulares para empoderar al personal

Fuente: Elaboraciòn Propia

2.2.4 Propuesta para mejorar la seguridad

Aunque no se han encontraron circunstancias desfavorables para sus sistemas informáticos, existen amenazas latentes como ataque inesperados o suplantaciones de su identidad corporativa.

En general su seguridad es buena, gracias a su monitoreo constante concatenando un control tanto físico como lógico en forma paralela a las bondades lógicas de sus activos computacionales.

El plan recomendable es:

- Adoptar una normativa de auditoria como COBIT o ISO para potenciar todas sus áreas e inculcar una filosofía de mejora continua
- Planificar los costos de mantenimiento, adquisición y actualización de equipos/software en el presupuesto anual
- Renovar ordenadores e infraestructura tecnológica periódicamente
- Migrar a sistemas operativos de licencia libre, debido a que son más seguros y cuentan con interfaces similares a Windows
- Comprar almacenamiento en la nube acorde al desarrollo de la empresa
- Adquirir un generador para evitar cortes repentinos de electricidad
- Auditar la empresa anualmente
- Retroalimentar las medidas mediante un hackeo ético para reforzar sus sistemas

3. CONCLUSIONES:

- La empresa Ferretería Armijos administra eficientemente sus recursos informáticos, no presenta ataques ni vulnerabilidades alarmantes, gestiona sus datos sistemáticamente al respaldarlos, procesarlos y supervisar al personal, quienes se sientes comprometidos con el crecimiento de la empresa.
- Es relevante notar que no existe una metodología de auditoria, aunque se tienen concepciones básicas y conjeturas preventivas, no se examina a fondo los sistemas lógicos ni su seguridad, esto se atribuye al retraso tecnológico de nuestra sociedad y falta de cultura en términos de protección de datos e informaciòn.
- Las auditorías informáticas son procesos que se llevan a cabo con el fin de evaluar el funcionamiento de un sistema informático, en donde verifican que tanto los equipos como los programas y aplicaciones funcionen con total normalidad, respondiendo satisfactoriamente a los

requerimientos de la empresa y utilizando el menor porcentaje de recursos en su desempeño.

4. REFERENCIAS BIBLIOGRÁFICAS

Arcentales Fernández, D., & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de las ciencias*, 157-173.

Caiza Acero, M., & Bolaños Burgos, F. (2014). Las implementaciones de las normas de seguridad de la información: estudio de caso la Sociedad de Lucha Contra el Cáncer del Ecuador. *Revista electrónica de Computación, Informática, Biomédica y Electrónica*, 2-19.

Cantos Ochoa, M. E. (2019). La auditoría integral como herramienta de validación de la gestión institucional. *Telos*, 1-19.

CompuTrabajo. (s.f.). *CompuTrabajo*. Obtenido de https://www.computrabajo.com.ec/empresas/acerca-de-ferrearmijos-sa-5D39CF30BC06C92D

Corda, M., Viñas, M., & Coria, M. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata)*, 1-18.

Díaz Ricardo, Y., Pérez del Cerro, Y., & Proenza Pupo, D. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. *Ciencias Holguín*, 1-14.

EMIS. (27 de enero de 2020). *EMIS*. Obtenido de https://www.emis.com/php/company-profile/EC/Ferrearmijos_SA_es_3977497.html

Escofet, A., Folgueiras, P., Luna, E., & Palou, B. (2016). Elaboración y validación de un cuestionario para la valoracion de proyectos de aprendizaje-servicio. *Revista Mexicana de Investigación Educativa*, 929-949.

Gil Vera, V. D., & Gil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*, 193-197.

Hernández Saucedo, A. L., & Mejia Miranda, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *Revista electrónica de Computación, Informática Biomédica y Electrónica*, 2-18.

Hernández, O. (2016). La auditoría interna y su alcance ético empresarial. *Actualidad Contable Faces*, 15-41.

López Vargas, Y., & Vázquez Chávez, A. (2016). La Gestión de Servicios de soporte técnico en el ciclo de vida del desarrollo de software. *Revista Cubana de Ciencias Informáticas*, 46-60.

Quiroz Zambrano, S., & Macías Valencia, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, 137-156.

Solana Álvarez, J. M. (2014). El sistema de información de una organización. Necesidad de implicación de la dirección. *Anuario Jurídico y Económico Escurialense*, 471-480.

Troncoso Pantoja, C., & Amaya Placencia, A. (2017). Entrevista: guía práctica para la recolección de datos cualitativos en investigación de salud. *Revista de la Facultad de Medicina*, 329-332.