UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA TECMESH UBICADA EN EL CANTÓN HUAQUILLAS PROVINCIA DE EL ORO

CABRERA FAJARDO SIXTO BENJAMIN
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORIA DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA TECMESH UBICADA EN EL CANTÓN HUAQUILLAS PROVINCIA DE EL ORO

CABRERA FAJARDO SIXTO BENJAMIN
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

FACULTAD DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORIA DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA TECMESH UBICADA EN EL CANTÓN HUAQUILLAS PROVINCIA DE EL ORO

CABRERA FAJARDO SIXTO BENJAMIN
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

GONZALEZ SANCHEZ JORGE LUIS

MACHALA, 26 DE AGOSTO DE 2019

MACHALA
26 de agosto de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado Auditoria de la seguridad informática en la empresa Tecmesh ubicada en el Cantón Huaquillas Provincia de El Oro, 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

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 2

ILLESCAS ESPINOZA WILMER HENRY
0704128776
ESPECIALISTA 3

Fecha de impresión: lunes 26 de agosto de 2019 - 06:56

URKUND

Urkund Analysis Result

Analysed Document: PROYECTO TITULACION SIXTO CABRERA.docx (D54792410)
Submitted: 8/13/2019 5:11:00 AM
Submitted By: sbcabrera_est@utmachala.edu.ec
Significance: 0 %

Sources included in the report:

Instances where selected sources appear:

0

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

El que suscribe, CABRERA FAJARDO SIXTO BENJAMIN, en calidad de autor del siguiente trabajo escrito titulado Auditoria de la seguridad informática en la empresa Tecmesh ubicada en el Cantón Huaquillas Provincia de El Oro, 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.

El autor 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.

El autor 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, 26 de agosto de 2019

CABRERA FAJARDO SIXTO BENJAMIN
0705373983

RESUMEN

La auditoría de seguridad informática se está promoviendo a nivel mundial, debido a las nuevas tecnologías que permiten el alcance de la información, los empresarios han acudido a estos tipos de auditoria para poder salvaguardar sus activos y de esta manera evitar que terceros se apropien de la información y cause daños generales; por esta razón la empresa Tecmesh se siente en la obligación de ser auditada para verificar la vulnerabilidades y riesgos que se enfrenta. La realización de este trabajo presenta una auditoria de seguridad enfocado en la búsqueda de riegos, vulnerabilidades y amenazas, en la cual se utilizó la metodología pragmática utilizando guías y matrices de evaluación que permite identificar y calificar los procesos, en consecuencia, se obtiene la información necesaria y suficiente que permite realizar un dictamen que se presenta al equipo administrativo para que puedan tomar decisiones que les permita salvaguardar su información. Los resultados revelan que existe la necesidad de un sistema informático contable para un mejor control de recursos y mejoramiento en el sistema eléctrico.

Palabras claves:

Seguridad informática, auditoria informática, riesgos informáticos, seguridad física, seguridad lógica.

ABSTRACT

The computer security audit is being promoted worldwide, due to the new technologies that allow the scope of the information, the businessmen have gone to these types of audits to be able to safeguard their assets and thus prevent third parties from appropriating the information and cause general damage. For this reason the Tecmesh company feels obligated to be audited to verify the vulnerabilities and risks it faces. The performance of this work presents a security audit focused on the search for risks, vulnerabilities and threats, in which the pragmatic methodology was used using guides and evaluation matrices that allow identifying and rating the processes, consequently the necessary information is obtained and enough to make an opinion presented to the administrative team so that they can make decisions that allow them to safeguard their information. The results reveal that there is a need for an accounting computer system for better control of resources and improvement in the electrical system.

Keywords: Computer security, Computer audit, Computer risks. physical security, logical security.

Contenido

INTRODUCCIÓN

En la última década la información automatizada está al alcance de todos, el funcionamiento de las empresas y el diario vivir de la población es un constante cambio de información, los gerentes son conscientes de la importancia de la tecnología tanto para la producción como para competir en el mercado, por este motivo siempre están en búsqueda de avances tecnológicos para implementar en sus empresas.

Los sistemas informáticos como cualquier otra herramienta tienen ventajas y también algunas amenazas como programas maliciosos, programación con errores, intrusos entre otros, que si no son tomados en cuenta en el momento oportuno pueden convertirse en complicaciones para la empresa, de ahí surge la necesidad de la seguridad informática.

La seguridad informática se enfoca en proteger los sistemas informáticos, es decir, la información que está en las computadoras y la información que circula mediante las redes, permite conocer la vulnerabilidad, riesgos y amenazas a las que pueden enfrentar.

Por ningún motivo se debe confundir la definición de seguridad informática y seguridad de la información en cambio la seguridad de la información está enfocada en la información en sí y se puede encontrar en diferentes medios, es activo de las empresas, estos son utilizados para la toma de decisiones estratégicas de la misma.

Es esencial en las organizaciones la implementación de auditoria de la seguridad informática para obtener mejoras como; desarrollo de las funciones, control de información, garantizar el perfecto estado de hardware, software.

Por lo mencionado anteriormente, mediante la presente investigación el objetivo es realizar una Auditoria de la seguridad informática a la empresa Tecmesh ubicada en la ciudad de Huaquillas, con la finalidad de analizar vulnerabilidades, riesgos y amenazas mediante una guía de evaluación para alcanzar los niveles de seguridad.

La metodología a implementar es el método pragmático, apoyado en las guías y matrices de evaluación como sugiere Muñoz, (2002).

1. FUNDAMENTACIÓN TEÓRICA

1.1. Auditoria

Auditoria según Escalante, (2014) es un proceso de verificación de información financiera, operacional o administrativa de la empresa, con la finalidad de tener la seguridad mediante evidencias que la empresa realiza sus funciones encaminadas a los requerimientos legales e institucionales con la finalidad de alcanzar las metas planificadas.

1.2. Auditoria Informática

Auditoria informática es el procedimiento que se realiza para evaluar la eficiencia y seguridad de los recursos informáticos, los resultados son emitidos en un informe que sirve para tomar decisiones adecuadas (Martínez , Blanco , & Loy, 2013).

1.3. Seguridad Informática

Seguridad informática permite proteger el sistema informático, minimizar riesgos y prevenir el acceso de información a terceros para uso malicioso o con fines económicos mediante estándares de seguridad (Gil & Gil , 2017).

Según Suárez & Ávila, (2015) Indican que la confidencialidad es una de las características fundamentales en la seguridad informática ya que permite salvaguardar y prohibir el acceso a la información a usuarios sin autorización.

1.4. Seguridad Física y lógica

Para Espinoza y Rodríguez, (2017) la seguridad física son todas las barreras que se implementan para controlar y prevenir amenazas físicas como inundaciones, incendios, entre otros, con la finalidad de resguardar el hardware y almacenamiento de datos, en cambio la seguridad lógica son todas las medidas que se toman para proteger la información y evitar el acceso a personas no autorizadas.

1.5. Fases de la Auditoria

La autoría consta de 3 fases: la primera es la planeación, donde se describe los pasos para realizar la auditoria además se establecen los objetivos, el personal encargado de calidad, los responsables del personal, fechas y cronogramas. (Escobar , Moreno, & Cuevas, 2016)

Luego en la fase de ejecución se reúnen el personal para verificar el plan, plantear los procedimientos, metodologías, recopilan información y se evalúa para luego presentarlos en la tercera fase que es informe, este documento se entrega al encardado de calidad de la empresa y el constara el resultado obtenidos de manera clara y sencilla, a la vez se indicaran medidas para mejorar si existe alguna falencia en la empresa.

1.6. Control Interno

El control interno Vega y Nieves, (2016) lo describe como un procedimiento en el que colaboran todos los trabajadores de la empresa con la finalidad de proveer una seguridad razonable mediante el cumplimiento de objetivos.

1.7. Vulnerabilidad informática

El termino vulnerabilidad representa ambientes expuestos a un ataque, debido a debilidades del sistema de información, permitiendo un libre acceso a terceras personas u otros sistemas informáticos pongan en peligro la confidencialidad e integridad de los datos y recursos de la empresa. (Monsalve, Aponte, & Chaves, 2014)

1.8. Riesgos informáticos

Riesgos informáticos son aquellos ataques causados por programas automatizados que permiten atacar y usurpar la información causando daños informáticos, también los hackers envían sistemas maliciosos como caballo de troya, y gusanos informáticos capaces de dañar todo un sistema o red informática. (Duque, Larry, & Renteria, 2011)

1.9. Delitos informáticos

De acuerdo a la teoría de Mayer, (2016) el delito informático se realiza con intención de provocar daños como pérdidas de datos, revelaciones confidenciales y alteraciones como bloqueos impidiendo el uso de los sistemas informáticos, estos son causados por personas malintencionadas que utilizan el software capaz de infiltrarse de manera silenciosa y acaparar toda la información.

1.10. Autenticación

La definición de Autenticación de usuarios de Sánchez y Enrique, (2017) es que su principal función es verificar la identidad y el rol sobre el sistema de información a utilizar brindando seguridad y autenticidad a la información a procesar.

1.11. Amenazas

Las amenazas son aquellos acontecimientos maliciosos capaces de perjudicar y alterar el sistema de información, causando daños materiales. Según Henarejos, y otros, (2014) Generalmente su ataque se realiza por medio de virus y programas silenciosos encargado de dañar y acaparar la información.

1.12. ISO 27001

La norma ISO 27001es una norma internacional creada con la finalidad de gestionar la seguridad, brindando una mejora continua, permitiendo crear confianza en la integridad de la información y en el negocio. La norma internacional puede ser empleada en cualquier tipo de negocio sea o no con fines de lucro, de esta manera genera seguridad a su información con la certificación que obtiene cumpliendo la normativa Arévalo, Bayona , & Dewar, (2015).

2. DESARROLLO

2.1. Metodología de la investigación de la Auditoria Informática

La metodología aplicada en la investigación es de tipo pragmático. Muñoz, (2002) especifica matrices y guía de evaluación que luego de recolectar información mediante técnicas como la observación a las instalaciones de la empresa y entrevista al gerente propietario y trabajadores, se analizan y evalúan para luego ser presentados en el informe con la finalidad de minimizar riesgo y obtener indicadores para la toma decisiones en la organización, el enfoque utilizado es pragmático.

2.2. Fase de planeación

2.2.1. Planeación de la auditoria

La empresa Tecmesh con numero de Ruc 1717338261001 con su representante legal Ing. Héctor Mena Cornejo, se constituye en el cantón de Huaquillas provincia de El oro el 23 de septiembre de 2013, ubicada en calle nueve de octubre s/n intersección Imbabura, se dedica como actividad principal a la comercialización de venta de servicio de internet, actualmente consta de 7 trabajadores: 2 secretarias en el aérea de ventas y 5 técnicos cumpliendo el rol de instalación y soporte del servicio. (Ver anexo N1 organigrama estructural)

2.2.2. Visita Preliminar al área auditada

Se realizo una entrevista con los colaboradores de la empresa, se formuló una serie de preguntas, la primera cuál es la misión y visión de su empresa, manifestando que no sabían, luego se preguntó el día que iniciaron sus labores, indicando que deben de leer

el manual de usuario para saber cuáles son las reglas que deben de seguir, la respuesta obtenida fue que al iniciar sus labores se indicaron tareas verbales, confirmando la inexistencia de un control interno.

En el departamento administrativo se evidenció que el manejo de una portátil Dell I5 séptima generación, el sistema de conexión a internet es inalámbrico, se detectó el cableado de red está en paralelo al sistema eléctrico. El sistema eléctrico no contiene conexión a tierra y no tiene un regulador de voltaje, la cámara de seguridad cubre toda el área de trabajo.

El área de atención al cliente consta de 3 computadores, dos reguladores, y un Ups, un switch de 8 líneas, la red de cableado está ocupando la superficie del suelo sin tener protección alguna. La máquina de escritorio es una I3 marca Lenovo, un monitor de 19 pulgadas marca Dell, los demás ordenadores son portátiles, de marca Dell i7 séptima generación.

Se evidencio que todas las computadoras que contiene la empresa Tecmesh están actualizadas con la última versión del Windows 10, tienen licencia original y sus aplicaciones de ofimática como el paquete de office están actualizado al presente año, no contienen un sistema contable ni contraseña los ordenadores asignados a cada empleado, trabajan en una hoja de Excel de manera general y su facturación es de manera manual.

La empresa cuenta con un departamento externo donde se encuentra ubicado el servidor y la distribución del internet de fibra óptica, cuenta con un UPS conectado a 4 baterías para generar energía de 6 horas cuando exista algún plan de contingencia y evitar corte de internet a los usuarios. Se evidencio que el cableado de fibra óptica no cuenta con un orden y están expuestos al riesgo.

En la siguiente matriz se detallará las características de las computadoras

TABLA 1. Características del Hardware

Número de computadoras	**4**
Observaciones:	1 portátil_ gerente
	1 pc escritorio área de ventas
	1 portátil secretaria
	1 portátil activadores-instalador de servicio
PC- escritorio	**Área ventas**

	Marca Lenovo
	procesador i3
	Intel® Core™ 2130 CPU @3.40 GHz-3.40 GHz
	Ram 8gb
	Disco duro 1tb
	Puertos USB: 3 puertos 3.0/3 puertos 2.0
Pc-portátil	**Gerente:**
	Marca Dell
	Procesador i5 séptima generación
	Intel®core™ 7200u CPU@2.50Ghz 2.70GHz
	ram: 12gb
	Disco Duro: 1Tb ssd marca Kingston
	Puertos USB: 3 puertos 3.0
	Secretaria-Instaladores
	Marca Dell
	Procesador i7 séptima generación
	Intel®core™ 7500u CPU@3.80Ghz
	ram: 12gb
	Disco Duro: 1Tb ssd marca Kingston
	Puertos Usb: 3 puertos 3.0
Periféricos de entrada	Mouse Fantech T530
	Teclado Fantech Hunter k10
	Pantalla Dell 19´´
Periféricos de salida	Impresora Epson l395

Fuente: Elaboración Propia.

Objetivo de la Auditoria Informática realizada a la Empresa Tecmesh

Aplicar una Auditoria de la seguridad informática a la empresa Tecmesh ubicada en la ciudad de Huaquillas, con la finalidad de analizar vulnerabilidades, riesgos y amenazas mediante una guía de evaluación para alcanzar los niveles de seguridad.

Objetivos específicos

Verificar la seguridad de los activos informáticos.

Verificar la existencia de un sistema contable.

Verificar y evaluar la existencia de seguridad a accesos de usuarios.

2.3. Guía de la Auditoria

TABLA 2. Matriz de la Auditoría

Actividades evaluar	Procedimiento de auditoría	Herramientas de auditoría
Verificación del hardware	Determinar el número de ordenadores	Observación
	Verificar característica del hardware	Observación, manipulación del hardware
	Verificación de regulador y UPS	Observación, manipulación de los dispositivos
	Verificación de la ficha técnica.	Revisión documental
Verificación de factores de entorno	Verificar el funcionamiento de los Aires acondicionados	Medidor de temperatura
	Verificar si la existencia Cámaras de seguridad	Observación
	Verificación del cableado eléctrico	Observación
	Verificación del cableado de red	Observación
Verificar control de acceso físico	Verificar que el usuario cumpla con la política de uso de contraseña	Entrevista con los usuarios
Verificar control de mantenimiento, preventivo y correctivo	Solicitar al aérea de mantenimiento la ficha técnica del mantenimiento de los ordenadores	Revisión documental
Verificar la actualización del software	Determinar si el sistema operativo esta actualizado con su respectiva licencia	Observación-manipulación del software

	Determinar si el ordenador cuenta con un antivirus y su respectiva licencia	Observación-manipulación del software
	Verificar el sistema contable de la empresa	Observación-manipulación del software
	Verificar si el paquete de office esta actualizado y consta con licencia	Observación-manipulación del software
Verificar la protección y respaldo de la información	Verificar si la información se respalda en un servidor Plan de contingencia	Entrevista con el gerente
Verificar la restricción a sitios web no permitido	Verificar que los equipos de cómputo tengan la restricción a páginas web no autorizadas	Observación-manipulación del software
Verificar capacitaciones al personal	Verificar si los usuarios tienen certificados de capacitaciones según el rol que es asignado	Entrevista al personal

Fuente: Elaboración Propia

2.4. Guía de evaluación

Tabla 3. Matriz de Evaluación.

Punto a evaluar	9-10	7-8	6-7
	Excelente	Suficiente	Deficiente
Verificación del hardware	El auditor verifico que el hardware utilizado está en excelente estado y actualizado para las operaciones necesarias para la empresa	el auditor verifico que el hardware utilizado es apto para las operaciones necesarias que requiere la empresa	el auditor verifico que el hardware utilizado es no es apto para las operaciones que requiere la empresa

Verificación de factores de entorno	el auditor verifico que los factores de entorno se encuentran en una adecuada ubicación y correcto funcionamiento	el auditor verifico que los factores de entorno están en buen funcionamiento	el auditor verifico y constato que los factores de entorno necesitan reacondicionar
Verificar control de acceso físico	el auditor verifico que las políticas establecidas se les indico a los usuarios desde el primer día de trabajo y se están cumpliendo por los usuarios	el auditor verifico que las políticas establecidas se están cumpliendo por los usuarios	el auditor verifico y constato que las políticas establecidas tienen que ser actualizadas a los requerimientos de la empresa
Verificar control de mantenimiento, preventivo y correctivo	el auditor verifico que los mantenimientos preventivos y correctivos se está haciendo de manera periódica	el auditor verifico la existencia de mantenimientos	el auditor verifico que no existe mantenimientos
Verificar la actualización del software	el auditor verifico que el software de los ordenadores está actualizado con su respectiva licencia y su funcionamiento es estable	el auditor verifico que el software esta actualizado y su funcionamiento es estable	el auditor verifico que el software instalado en los ordenadores no cumple con los requisitos necesarios
Verificar la protección y respaldo de la información	el auditor verifico que los sistemas de información cuentan con un servidor de respaldo y plan de	el auditor verifico que los sistemas de información cuentan con respaldo y soporte	el auditor verificó que los sistemas de información no cuentan con un plan de contingencia; no

	contingencia ante algún imprevisto		tienen respaldo de información
Verificar la restricción a sitios web no permitido	el auditor verifico que los ordenadores de cada departamento cuentan con un bloquea a sitios web no permitidos	el auditor verifico que los ordenadores de cada departamento cuentan con un bloquea a sitios web no permitidos	el auditor verifico que los ordenadores están libres para el uso de toda página web
Verificar capacitaciones al personal	el auditor verifico que el personal está capacitado acorde a su rol asignado	el auditor verifico que el personal está capacitado	el auditor verifico que el personal no está capacitado.

Fuente: Elaboración Propia

2.5. Resultados

A continuación, se detallará la evaluación realizada a la empresa Tecmech, con los siguientes hallazgos encontrados.

La empresa cuenta con 1 computador de escritorio y 3 portátiles dando un total de 4 computadoras.

Los ordenadores están con el hardware actualizado.

Los reguladores de voltaje y Ups se encuentran en excelente funcionamiento.

Los ordenadores no cuentan con ficha técnica, que detalla el hardware y el soporte realizado.

Los aires acondicionados están en perfecto estado, manteniendo a los equipos que se expongan a recalentamientos.

La empresa tiene 6 cámaras de seguridad masca Hik visión 1080 p, 4 tipo domo en la parte interna y 2 tubo en la parte externa de la empresa, su dvr es ampliable a 16 cámaras, se verifico que el enfoque por su ubicación es adecuado. la cablería se encuentra en desorden.

El cableado eléctrico está expuesto y se observa ausencia de instalación de varilla de cobre.

El cableado de red se encuentra en paralelo con el sistema eléctrico. Puede provocar ruido y perdida de datos.

Se verifico la ausencia de un control interno.

Los mantenimientos realizados son detallados en un cuaderno, se procede constatar última fecha de mantenimiento. Se confirma que los equipos constan con mantenimientos preventivos.

El sistema operativo esta actualizado a su última versión con su respectiva licencia, y su configuración está en el máximo rendimiento.

Las computadoras no cuentan con un sistema de antivirus.

Ausencia de sistema contable, la información de sus clientes se encuentra en agendas y en una hoja electrónica de Excel.

El paquete el office se encuentra actualizado con su respectiva licencia.

Los datos registrados en el ordenador, son respaldos en un servidor externo de la entidad.

Los equipos de cómputo, no cuentan con restricción a páginas web no autorizadas.

El personal se encuentra cuenta con un nivel de capacitación actualizada, sus niveles académicos son de tercer nivel.

2.6. Dictamen

Con los resultados obtenidos en el proceso de evaluación me permito comunicarle las siguientes observaciones y recomendaciones.

Se evidencia que los ordenadores de cada departamento se encuentran actualizados, con un sistema operativo Windows 10 con sus respectivas licencias, cuenta con un paquete de ofimática Microsoft office 2019 con su respectiva licencia vigente, no cuenta con un antivirus virus, esto hace que los ordenadores estén expuestos a ataques y se pierda la información, provocando un riesgo a los ordenadores, se recomienda instalar un sistema de antivirus actual con su respectiva licencia, (Ejem. Eset Protección total).

Se detecto ausencia del sistema de contable, la empresa lleva los registros en cuaderno y en hojas de cálculo Excel, no cuentan con un Kardex para las existencias del

inventario. El computador designado para los registros de contabilidad no cuenta con una contraseña, se recomienda adquirir un sistema informático contable.

Se detecto desorden en la cablería eléctrica, está expuesta a la intemperie y no consta instalación varilla de cobre, esto puede provocar que el hardware sufra daños de reparación o pérdida total, se recomienda contratar un electricista para que realice una inspección y proforma para la reubicación y organización del cableado eléctrico.

Se detecto que la instalación de red con cable UTP en el área de ventas está en paralelo con los cables de electricidad, esto puede provocar ruido y perdida de datos, se recomienda que se debe reestructurar el sistema de red.

Se procede recomendar a la empresa Tecmesh implementar de manera inmediata el control interno, este le permite a la organización tener un orden, control y aumentar la eficiencia en el trabajo además le permite salvaguardar los recursos.

3. CONCLUSIONES

Luego haber realizado la Auditoria Informática en la Empresa Tecmesh se puede concluir que existen algunas falencias:

1. Los equipos de computo se encuentran en excelente estado y cumplen con los requisitos técnicos apropiados para su funcionamiento, en cuanto al sistema eléctrico existen falencias que podrían ocasionar futuros problemas.
2. La usencia de un sistema informático contable tiene como consecuencia perdida y desconocimiento de información, inexistencia del estado actual de la empresa, provocando un difícil control de la empresa.
3. Es necesario la implementación de un Auditor Interno, que verifique el correcto cumplimiento de las funciones de trabajadores, los procesos y todas las áreas de la empresa con el fin de estructurar un control interno acorde a las necesidades que requiere; permitiendo alcanzar la eficiencia.

Referencias

Analytics Software & Solutions. (s.f.). Recuperado el 2019, de https://www.sas.com/search/en_us.html?q=sas%20enterprice

Arévalo, J., Bayona , R., & Dewar, R. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001:. *Tecnura*. Obtenido de https://www.redalyc.org/articulo.oa?id=257042318011

Duque, J., Larry, A., & Renteria, E. (2011). Análisis omparativo de las principales técnicas de hacking empresarial. *Scientia et Technica*. Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/2518/0058S586_anexo.pdf?sequence=2

Escalante, P. (28 de Enero de 2014). Auditoría financiera: Una opción de ejercicio profesional independiente para el Contador Público. *Actualidad Contable Faces, 17*. Obtenido de http://www.redalyc.org/articulo.oa?id=25731098004

Escobar , D., Moreno, M., & Cuevas, L. (2016). La calidad de la auditoría en Sistemas de Gestión. Software AUDIT_INTEGRATED. *Ciencias Holguín*. Obtenido de http://www.redalyc.org/articulo.oa?id=181545579007

Espinoza , E., & Rodríguez, R. (2017). Seguridad informática una problemática de las organizaciones en el sur de Sonora. *Revista de Investigación Academica sin Frontera*. Obtenido de http://revistainvestigacionacademicasinfrontera.com/sistema/index.php/RDIASF

Gil , V. V., & Gil , J. V. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica*. Obtenido de http://www.redalyc.org/articulo.oa?id=84953103011

Henarejos, A., Fernández, J., Toval, A., Hernández, I., Sánchez, A., & Carillo, J. (2014). Guía de buenas prácticas de seguridad informática en tratamiento de datos de salud para el personal sanitario en atencion primaria. *El sevier doyma*. Obtenido de https://www.sciencedirect.com/science/article/pii/S0212656714000067?via%3Dihub

Martínez , Y., Blanco , B., & Loy, L. (2013). Propuesta del Sistema de Acciones para la implementación de la Auditoría con Informática. *Revista de Arquitectura e Ingeniería*. Obtenido de http://www.redalyc.org/articulo.oa?id=193929227003

Mayer , L. (2016). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*. Obtenido de https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122018000100159&lang=es#fn200

Monsalve, J., Aponte, F., & Chaves, D. (2014). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007&lang=es

Muñoz, C. (2002). *Auditoria en sistemas computacionales.* México: Pearson.

Sánchez, J., & Enrique, J. (2017). Riesgos de ciberseguridad en las empresas. *Revista de Ciencia, tecnologia y medio ambiente*. Obtenido de https://revistas.uax.es/index.php/tec_des/article/download/1174/964

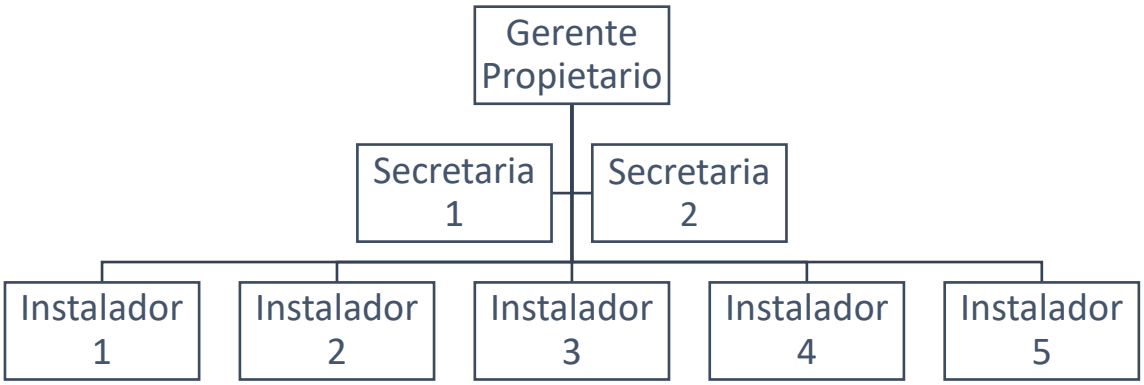
Suárez, D., & Ávila, A. (2015). Una forma de interpretar la seguridad informática. *Journal of Engineering and Technology*. Obtenido de http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015/1072

Vega , L., & Nieves, J. (2016). Procedimiento para la Gestión de la Supervisión y Monitoreo del Control Interno. *Ciencias Holguín*. Obtenido de http://www.redalyc.org/pdf/1815/181543577007.pdf

ANEXOS

Anexo A.

Organigrama Estructural



Fuente: Elaboración Propia