UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA CUESGAR S.A, UBICADA EN EL CANTÓN EL GUABO, PARROQUIA TENDALES.

NEIRA CUEVA CRISTHIAN XAVIER
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA CUESGAR S.A, UBICADA EN EL CANTÓN EL GUABO, PARROQUIA TENDALES.

NEIRA CUEVA CRISTHIAN XAVIER
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA CUESGAR S.A, UBICADA EN EL CANTÓN EL GUABO, PARROQUIA TENDALES.

NEIRA CUEVA CRISTHIAN XAVIER
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

ORDÓÑEZ BRICEÑO KARLA FERNANDA

MACHALA, 04 DE FEBRERO DE 2019

MACHALA
04 de febrero de 2019

Nota de aceptación:

Quienes suscriben, en nuestra condición de evaluadores del trabajo de titulación denominado AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA CUESGAR S.A, UBICADA EN EL CANTÓN EL GUABO, PARROQUIA TENDALES., 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.

ORDÓÑEZ BRICEÑO KARLA FERNANDA
0705031003
TUTOR - ESPECIALISTA 1

GONZALEZ SANCHEZ JORGE LUIS
0703333898
ESPECIALISTA 2

CHIMARRO CHIPANTIZA VICTOR LEWIS
0703703413
ESPECIALISTA 3

Fecha de impresión: lunes 04 de febrero de 2019 - 07:51

URKUND

Urkund Analysis Result

Analysed Document: NEIRA CUEVA CRISTHIAN XAVIER_PT-011018.pdf (D47131340)
Submitted: 1/22/2019 11:08:00 PM
Submitted By: titulacion_sv1@utmachala.edu.ec
Significance: 1 %

Sources included in the report:

Recalde_Espinosa_Angel_Francisco.docx (D40253986)

Instances where selected sources appear:

1

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

El que suscribe, NEIRA CUEVA CRISTHIAN XAVIER, en calidad de autor del siguiente trabajo escrito titulado AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA CUESGAR S.A, UBICADA EN EL CANTÓN EL GUABO, PARROQUIA TENDALES., 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, 04 de febrero de 2019

NEIRA CUEVA CRISTHIAN XAVIER
0707070934

RESUMEN

El presente estudio se enfoca en la auditoría de seguridad informática en la empresa "CUESGAR S.A." debido a la gran importancia que tiene la actualidad determinar el correcto desempeño de los recursos informáticos, debido a que son necesarios para obtener información fiable, eficiente y segura dentro de la organización. El objetivo propuesto es analizar las vulnerabilidades, amenazas y riesgos que poseen los equipos informáticos de la empresa, mediante la aplicación de herramientas y métodos para emitir controles de seguridad necesarios para resguardar los activos. La metodología empleada es la auditoria de sistemas computacionales (ASC) la cual se enfoca en tres etapas; la primera etapa es la planeación la cual permite definir las actividades que se efectuarán en el proceso de auditoría, consecutivamente la etapa a desarrollar es la ejecución en donde se obtendrá la información confidencial de acuerdo a las herramientas utilizadas, y en la última etapa que es el dictamen se indica la opinión del auditor acerca de los hallazgos que fueron encontrados. Los resultados obtenidos permitirán identificar la seguridad que tiene la empresa en lo que corresponde a proteger y administrar la información, asimismo observar aquellas falencias que necesitan ser mejoradas con la finalidad de cumplir eficientemente sus actividades.

Palabras Claves: Auditoría informática, vulnerabilidades, riesgos, amenazas y controles.

ABSTRACT

The present study focuses on the computer security audit in the company "CUESGAR SA" due to the great importance that currently has to determine the correct performance of the computer resources, because they are necessary to obtain reliable, efficient and safe information within of the organization. The proposed objective is to analyze the vulnerabilities, threats and risks that the company's computer equipment possesses, by applying tools and methods to issue security controls necessary to safeguard the assets. The methodology used is the audit of computer systems (ASC) which focuses on three stages; the first stage is the planning which allows defining the activities that will be carried out in the audit process, consecutively the stage to be developed is the execution where the confidential information will be obtained according to the tools used, and in the last stage that is The opinion indicates the auditor's opinion about the findings that were found. The obtained results will allow to identify the security that the company has in what corresponds to protect and manage the information, as well as to observe those deficiencies that need to be improved in order to efficiently fulfill their activities.

Keywords: Computer audit, vulnerabilities, risks, threats and controls.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

En la actualidad con el avance de la tecnología las empresas se encuentran expuestas a vulnerabilidades y ataques informáticos que tienen como fin acceder a la información confidencial de la institución y hacer un mal uso de la misma, debido a los escasos controles implementados en lo que corresponde a la seguridad física y lógica, por ello es importante que cada entidad establezca medidas de seguridad que permitan proteger uno de los activos más importante que es la información (Gil V & Gil J, 2017). En lo que respecta al Ecuador también existen delitos informáticos y robos de contraseñas, por ello se indica que este tipo de problemas se presenta a nivel mundial (López, 2017).

Mediante la aplicación de auditorías de seguridad informática en las empresas permiten obtener un diagnóstico de los sistemas operativos y recursos informáticos, detallando las vulnerabilidades, amenazas y riesgos que se encuentran expuestos dentro de la institución (Vega & Ramos, 2017). Para reducir las falencias de las entidades es necesario aplicar controles de seguridad para evitar la pérdida de información.

Por lo mencionado anteriormente el presente trabajo investigativo se encuentra relacionado en aplicar una auditoría de seguridad informática en la Empresa "CUESGAR S.A" con el objetivo propuesto de analizar las vulnerabilidades, amenazas y riesgos que poseen los equipos informáticos de la empresa, mediante la aplicación de herramientas y métodos para emitir controles de seguridad necesarios para resguardar los activos.

El enfoque de la investigación fue de carácter descriptivo, debido a que se empleó la metodología para realizar auditoría de sistemas computacionales (ASC) propuesta por Muñoz, (2002), el cual sirvió como guía para establecer ciertos pasos para el desarrollo del objeto de estudio. El proceso de auditoría consiste en las etapas de planeación, ejecución y el dictamen de acuerdo a los hallazgos encontrados dentro del proceso de auditoría. De la misma manera, fue necesario determinar tres puntos a evaluar los cuales se encuentran relacionados con las políticas y el manejo del programa contable, las funciones y actividades del personal y la evaluación de las operaciones físicas y lógicas de la empresa.

1. FUNDAMENTACIÓN TEÓRICA

1.1 Seguridad Informática

La seguridad informática se encarga de proteger los activos que cuentan las organizaciones con el fin de minimizar las vulnerabilidades que se pueden presentar, por ello es necesario aplicar controles que permiten asegurar la integridad y confidencialidad de la información (Suarez & Ávila, 2015). Por lo consiguiente, mediante la aplicación de mecanismos eficientes los sistemas informáticos funcionaran correctamente. El objetivo principal que tiene la seguridad informática, es reducir al mínimo los riesgos informáticos que se pueden encontrar expuestos las organizaciones, proporcionando así que la información sea confiable (Quiroz & Macías, 2017).

1.2 Ataques Informáticos

Son acciones que tienen como propósito causar daño o problemas al sistema informático, los cuales pueden ser realizado por una persona o grupo de personas que buscan obtener un beneficio de la información que acceden. Existen dos clases de ataques; los ataques pasivos consisten en la obtención de la información para ser utilizada indebidamente o ser divulgada, en cambio, en lo que respecta a los ataques activos son aquellos que cambian los flujos de información (Guevara, 2018).

1.3 Vulnerabilidades

Se denominan vulnerabilidades a las debilidades que se presentan en los sistemas informáticos, los cuales pueden comprometer la seguridad de la información (Serrato, 2016). Las vulnerabilidades que tienen mayor ocurrencia en las empresas son aquellas que se presentan debido a una mala configuración de los sistemas o por políticas de seguridad ineficientes (Gomez, Medina, Jiménez, Gómez, & Sánchez, 2017).

1.4 Amenazas

Las amenazas son acciones de consecuencia negativa que pueden ocurrir en las empresas produciendo daños en los activos. Los tipos de amenazas que se presentan dentro de las organizaciones son virus informáticos, códigos maliciosos y los usos no autorizados de la información (Sánchez, et al, 2014).

1.5 Riesgos

Los riesgos se presentan posteriormente de la materialización de las vulnerabilidades y amenazas, es decir en primer lugar se identifica las vulnerabilidades que puede tener un sistema informático, posteriormente se convierte en amenaza debido a los fallos que se pueden presentar, para en lo consiguiente ser denominado como riesgo, que es cuando esta acción puede afectar las operaciones empresariales y su reputación (Santiago & Sánchez, 2017).

1.6 Controles de seguridad

Los controles de seguridad son medidas que se deben utilizar para llevar un control de accesos de los recursos empresariales. De la misma manera, es importante establecer políticas de seguridad que indiquen las directrices que se deben seguir para proteger los activos de las empresas, evitar el mal uso de la información y también estrategias para cumplir los objetivos propuestos por la alta dirección (Chilán & Ponce, 2017).

Los Controles preventivos sirven para reducir la probabilidad de que una acción negativa, ocurra en la empresa ocasionando pérdidas o daños de la información por ello, se implementan acciones de seguridad. De igual manera, tenemos los controles detectivos los cuales permiten establecer controles que identifiquen cuando se presenta una irregularidad y al momento de materializarse ser solucionadas inmediatamente, también este tipo de controles se caracterizan por que sirven para verificar que los controles preventivos están funcionando correctamente. El último de los controles existentes es el correctivo, el cual surge cuando los dos controles mencionados anteriormente son vulnerados, por lo que es necesario tomar medidas que permitan revertir un evento no deseado. Un ejemplo de este control es la recuperación de información mediante la implementación de copias de seguridad (González, Myer, & Pachón, 2017).

1.7 Seguridad física y lógica

La seguridad física radica en la protección de los recursos informáticos, mediante la aplicación de procedimientos que permitan garantizar el debido cuidado del hardware. Las principales amenazas físicas que se presentan dentro de una institución es el robo o las inundaciones causadas por fenómenos naturales (Espinoza & Rodríguez, 2017).

En lo que corresponde a la seguridad lógica consiste en la protección de los programas y aplicaciones que deben ser utilizada por el personal dentro de la empresa. Para ello se emplea controles que permitan que la información mantenga su integridad, confidencialidad y disponibilidad, como ejemplo tenemos; el encriptamiento y la autenticación de usuarios (Martelo, Tovar, & Maza, 2018)**.**

2. DESARROLLO

2.1 Metodología

El trabajo investigativo tiene un enfoque descriptivo, debido a que el auditor realizará un dictamen acerca de los hallazgos que se encontraron. Por ello, para la obtención de la información se tomará como referencia aquellos puntos relevantes para realizar la auditoria de sistemas computacionales (ASC).

En lo que corresponde a la planeación de la auditoría, se efectuará la visita preliminar, asimismo se plasmarán los objetivos de la auditoría. También es necesario indicar los puntos a evaluar y especificar las herramientas para la obtención de información. En la ejecución de la auditoría, se emplearán los instrumentos necesarios para determinar la seguridad informática para posteriormente emitir un dictamen, en el cual se indicará las situaciones encontradas y las recomendaciones que deben seguir (Muñoz, 2002).

2.2 Auditoría de Seguridad Informática

Por lo consiguiente, las etapas propuestas servirán para analizar el problema que se presenta en el centro de cómputo de la empresa “CUESGAR S.A” debido a que ha sufrido de varios ataques informáticos. ¿Por lo cual el gerente de la empresa necesita conocer las vulnerabilidades, amenazas, riesgos del centro de cómputo y los controles de seguridad que se deberían implementar para evitar ser víctimas de los ataques informáticos?

2.3 Planeación de la auditoría

2.3.1 Visita preliminar

En la visita preliminar que se efectuó a la empresa "CUESGAR S.A" se pudo conocer que cuentan con cuatro computadoras las cuales tiene internet, igualmente poseen un software contable denominado Sofadcon, pero no cuenta con políticas específicas donde indique las medidas de seguridad y manejo del sistema informático que se deben aplicar. Asimismo, se evidencio que todo el personal posee la clave y usuario de cada uno de ellos, lo cual no es pertinente debido a que puede ocasionar que la información sea utilizada de mala manera, modificándose o dando información a la competencia.

En lo que corresponde al cableado de las computadoras se evidencio que se encuentran mal ubicados debido a que la mayoría de los cables se encuentran el piso, lo cual puede ocasionar que algún trabajador los pise, o se enrede en ellos ocasionando la pérdida y deterioro del equipo.

Igualmente es importante indicar las especificaciones de las computadoras en lo que respecta al software, es decir el número de computadoras que cuenta la empresa, el pc, los periféricos de entrada, de la misma manera el hardware detallando el sistema operativo, paquete ofimático, programa contable.

Tabla 1: Especificaciones de las computadoras

Especificaciones de las computadoras			
Hardware		**Software**	
Número de computadoras	• 4	Sistema Operativo	• Microsoft Windows 8
PC	• Disco Duro 320 GB • Unidad CD-ROM • Memoria RAM 4 GB • Procesador Intel Core i3-2100	Paquete Ofimática 2016	• Microsoft Word • Microsoft Excel • Microsoft Power Point • Microsoft Access • Microsoft Publisher • Microsoft Outlook
Periféricos de entrada	• Teclado Genius • Mouse Genius • Impresora EPSON	Programa Contable	• Sofadcon
Router	• Router inalámbrico N 300 Mbps	Otros programas	• Antivirus Avast • Skype

Elaborado por: El autor

2.3.2 Objetivos de la auditoría

Objetivo General

- Efectuar la auditoría de seguridad informática en la Empresa "CUESGAR S.A" mediante la aplicación de herramientas y técnicas para determinar la seguridad que poseen acerca de sus activos.

Objetivos Específicos

- Analizar las políticas y manejo del programa contable mediante la indagación y observación para que se verifique si están correctamente planteadas.
- Verificar los conocimientos del personal de la empresa mediante la utilización de herramientas dirigidas al administrador para determinar sus competencias y habilidades.
- Identificar que el sistema operativo tenga su respectiva licencia con el análisis de la información que poseen las computadoras para cumplir eficientemente las actividades empresariales.
- Revisar la información proporcionada en los correos electrónicos mediante el análisis del mismo para comprobar que no se brinde datos confidenciales de la empresa.

2.3.3 Puntos a evaluar al centro de cómputo de la Empresa "CUESGAR S.A"

Políticas y manejo del programa contable

- Documentación de las políticas
- Socialización periódica de las políticas
- Verificación de contraseñas

Funciones y actividades del personal

- Cumplimiento de actividades por parte de los empleados
- Conocimiento y destreza del personal

Operaciones físicas y lógicas

- Antivirus

- Sistema operativo
- Correos electrónicos

2.3.4 Identificar y seleccionar métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría.

En el correspondiente proceso de auditoría realizado en la Empresa "CUESGAR S.A" es necesario elaborar una guía de auditoría en donde se detallarán las actividades a evaluar (Ver Anexo A), los procedimientos que se llevarán a cabo y las herramientas a utilizar. También es importante efectuar una matriz de evaluación (Ver Anexo B), en donde se describen los criterios de calificación.

Asimismo, se estableció las herramientas que se utilizarán en el proceso de auditoría, también el método que se empleará para obtener la información suficiente es el cuestionario, el cual se encuentra dirigido tanto para el personal y gerente de la empresa, de igual manera se realizará la ficha de observación.

2.4 Ejecución de la auditoría

Luego de establecer la primera de etapa planeación, es necesario llevar a cabo la ejecución en donde es importante plasmar las herramientas que fueron designadas en la guía de auditoría, las cuales son importantes para obtener la suficiente evidencia que permita posteriormente emitir una opinión acerca de la situación actual de la empresa en lo que respecta a la seguridad informática. Los instrumentos ejecutados fueron los siguientes:

- Cuestionario dirigido al personal y al gerente de la empresa (Ver Anexo C)
- Ficha de Observación (Ver Anexo D)

Consecutivamente aplicadas las herramientas, se realizará la matriz de resultados con aquellos hallazgos encontrados en la auditoría, en donde se determina el nivel de cumplimiento que tuvo la empresa de acuerdo a los tres puntos a evaluar establecidos en la guía. (Ver Anexo E)

De la misma forma, se estableció una matriz de riesgo en donde se establecen los factores de riesgos que mayor significancia, detallando el impacto y la probabilidad que tienen de ocurrir en la organización. (Anexo F)

Tabla 2: Análisis FODA

Fortalezas	**Oportunidades**
Las políticas que cuenta la empresa se encuentran documentadas.	Mantener las políticas documentadas es muy importante porque permite establecer que acciones realizar de acuerdo al proceso a seguir, por ellos es necesario que las misma detallen sistemáticamente las pautas que se deben efectuar.
El personal de la empresa cuenta con experiencia en el manejo de programas contables.	El conocimiento que el personal tenga en manejo de software contables es importante porque permite la adaptación y el correcto funcionamiento del mismo. Asimismo, es necesario brindar capacitaciones a los trabajadores para que fortalezcan sus habilidades y destrezas en beneficio de la institución.
Debilidades	**Amenazas**
Las políticas de manejo de la seguridad de la información se encuentran generalizadas.	Debido a que la información no es detallada sistemáticamente influye en que no se realice eficientemente las actividades, poniendo en riesgo el funcionamiento de la empresa.
Poca seguridad en las contraseñas de ingreso al programa contable.	El intercambio de clave entre trabajadores no es recomendable por la razón que al existir acceso a otros usuarios puede ser modificada y alterada la información, la cual perjudica la seguridad informática de la empresa.
Antivirus desactualizado	Al poseer antivirus desactualizados existe la posibilidad de que la información se pierda o se dañe debido a la inexistente protección que tienen las computadoras.
Poco cuidado en la información que se brinda mediante la utilización de correos electrónicos	Es importante tener en cuenta que al momento de proporcionar información confidencial de la empresa se corre el riesgo de que la misma sea mal utilizada, dañando así la sostenibilidad empresarial.

Elaborado por: El autor

2.5 Dictamen de la auditoría

Machala, 02 de enero de 2019

Sra. Vilma María García
Administradora de la Empresa "CUESGAR S.A"

De acuerdo a la auditoría de seguridad informática aplicada a la Empresa "CUESGAR S.A". El proceso de auditoría tuvo su inicio el día lunes 17 de diciembre del 2018. A continuación, se detallarán los resultados encontrados:

Punto a evaluar 1: Políticas y manejo del programa contable

- Se evidencio que existen políticas que determinan los procesos que se deben seguir en el programa contable, pero analizando la información se determina que se encuentra muy generalizada. Asimismo, es importante indicar que las políticas son socializadas cuando el personal ingresa por primera vez a laborar en la empresa y también es comunicada mediante la utilización de correos electrónicos.
- Las contraseñas que poseen los trabajadores al ingresar al programa contable es de conocimiento de cada una de las personas que tienen acceso.

Punto a evaluar 2: Funciones y actividades del personal

- El personal de la empresa cuenta con experiencia de tres años en el manejo de programas contables, de igual manera cumplen con las actividades que le indican la empresa, pero existen actividades que deben mejorar para trabajar eficientemente.

Punto a evaluar 3: Operaciones física y lógicas

- Los antivirus de las computadoras se encuentran desactualizados lo cual pone en riesgo la seguridad de la información, el sistema operativo que tiene la empresa es el Windows 8 pero no tiene licencia. En lo que respecta a los correos electrónicos se evidencio que no existe un control con la información que es proporcionada.

Por todo lo mencionado anteriormente, es necesario indicar las siguientes recomendaciones las cuales permitirán tener una mayor seguridad y evitar los ataques informáticos.

Punto a evaluar 1: Políticas y manejo del programa contable

- Al administrador de la empresa se le recomienda que establezca junto al contador las políticas específicas y sistemáticas que deben seguir los demás trabajadores para manejar eficientemente el programa contable. Además, es importante, que las políticas se socialicen constantemente para cumplir lo mencionado en las mismas.
- Las contraseñas del personal deben ser de uso exclusivo de ellos y no debe ser proporcionado a los demás trabajadores, el administrador de la empresa debe sancionar aquellos que incumplan esta acción, además se recomienda que las contraseñas tengan un alto nivel de seguridad.

Punto a evaluar 2: Funciones y actividades del personal

- Es importante establecer por parte del administrador, que el personal que tendrá acceso al software contable cuente con la experiencia necesaria en el manejo del programa.

Punto a evaluar 3: Operaciones físicas y lógicas

- Los antivirus de las computadoras se deben actualizar constantemente para proteger la información de la empresa y evitar que se contagie de virus. También es importante que posean la licencia del sistema operativo para ello es necesario realizar un presupuesto para identificar los desembolsos que son necesarios realizar. Se recomienda que antes de contestar mensajes mediante la utilización de correos electrónicos se debe tener cuidado de no proporcionar información confidencial.

Atentamente

_____

Cristhian Neira
Auditor

Tabla 3: Matriz de situaciones encontradas

Empresa: "CUESGAR S.A" **Área auditada**: Centro de cómputo **Fecha:** 02/01/2019

No.	Puntos evaluados	Causas	Solución	Responsable
1	Las políticas se socializan únicamente al ingreso de un trabajador y de vez en cuando se envían por correo electrónico modificaciones que se efectúan en las politicas.	Poca preocupación por socializar las políticas.	Determinar que las políticas de manejo y seguridad del programa contable se realicen constantemente y se utilicen el correo electrónico para indicar las actualizaciones que se realicen.	Administrador – Contador
2	Las políticas se encuentran documentadas pero no definen correctamente los procesos a seguir, es decir se encuentran generalizadas.	No realizan correctamente las políticas especificando los pasos a seguir.	Detallar paso a paso las políticas de manera que permitan realizar eficientemente las actividades garantizando el cumplimiento de los objetivos institucionales.	Administrador – Contador
3	Las claves y usuarios para ingresar al sistema contable, son de conocimiento de todo el personal de la empresa	No se ha establecido una política para no incurrir en esta acción	Establecer una política que cada trabajador debe guardar discreción con su usuario y clave. En caso de identificar una irregularidad recibirá una sanción económica.	Administrador
4	El cumplimiento de las actividades por parte del personal es regular.	Se comete errores debido a que no se especifican correctamente las acciones a realizar en las politicas.	En las politicas indicar correctamente los procesos que deben seguir los trabajadores, con el fin de garantizar el eficiente desempeño de sus actividades.	Administrador

5	El personal de la empresa posee tres años de experiencia en lo que respecta al manejo de software contables.	Debido a que los trabajadores en su mayoría son jóvenes.	Brindar capacitaciones para reforzar los conocimientos y habilidades de sus trabajadores.	Administrador
6	Las computadoras no poseen antivirus actualizados.	Poca atención en lo que corresponde a la actualización de antivirus.	Contar con el Antivirus Avast actualizados, para ellos es necesario establecer el monto necesario para realizar dicha acción.	Administrador
7	La empresa cuenta con el Sistema operativo Windows 8, pero sin licencia.	Debido a que no han tomado en cuenta esta situación dentro de la empresa.	Realizar un presupuesto para contratar la licencia del sistema operativo.	Administrador - Contador
8	Poco cuidado al momento de responder correos electrónicos, es decir se encuentran expuesto a proporcionar informacion confidencial.	El personal no conoce los riesgos que pueden ocasionar proporcionar informacion sin saber si son fuentes confiables.	Tener más cuidado al momento de brindar informacion y tratar de verificar la autenticidad de los correos electrónicos.	Trabajadores

CONCLUSIONES

Debido a la auditoría de seguridad informática realizada en la Empresa “CUESGAR S.A” se detectó que la empresa cuenta con vulnerabilidades como es la desactualización del antivirus, los cuales pueden ocasionar la pérdida de información o ralentizar las actividades operacionales asimismo el sistema operativo no cuenta con su respectiva licencia, De igual manera, se evidencia que la empresa cuenta con amenazas relacionadas a la utilización de correos electrónicos debido a que el personal no tiene cuidado con la información que se proporciona, lo cual puede afectar de manera económica y reputacional a la entidad. Otro punto a tomar en cuenta es el conocimiento de usuarios y claves que tienen todos los trabajadores al momento de ingresar al programa contable lo que no es recomendable debido a que se puede modificar, alterar o vender datos confidenciales de la institución. Por todo lo mencionado, se identificó que la empresa se encuentra expuesta a riesgos en la información lo cual puede ocasionar problemas económicos.

Por ello es necesario establecer controles de seguridad con la finalidad de que permitan proteger eficientemente los activos de la empresa. En lo que corresponde al sistema operativo, es importante establecer un presupuesto para llevar a cabo la mejora de la licencia. También es fundamental que se profundicen las políticas respecto al acceso y seguridad del software contable. Por ello, teniendo en cuenta los hallazgos encontrados y poniendo en práctica las recomendaciones que se detallaron en el dictamen de la auditoría por parte del administrador, contador y trabajadores permitirá mejorar la seguridad informática.

BIBLIOGRAFÍA

- Chilán, E., & Ponce, W. (2017). Apuntes teóricos introductorios sobre la seguridad de la información. *Revista Científica Dominio de las Ciencias, 3*(4), 284-295. Obtenido de http://dominiodelasciencias.com/ojs/index.php/es/article/view/686/762

- Espinoza, E., & Rodríguez, R. (2017). Seguridad informática una problemática de las organizaciones en el sur de Sonora. *Revista de Investigación Académica sin Fronteras*(25), 1-31. Obtenido de http://revistainvestigacionacademicasinfrontera.com/sistema/index.php/RDIASF/article/view/140/138

- Gil V, V., & Gil J, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia Et Technica, 22*(2), 193-197. Obtenido de http://revistas.utp.edu.co/index.php/revistaciencia/article/view/11371/10511

- Gomez, F., Medina, J., Jiménez, R., Gómez, J., & Sánchez, M. (2017). Plataforma Experimental para el Estudio de la Vulnerabilidad Hardware en los Robots Móviles: el Bus I2C como Caso de Estudio. *Revista Iberoamericana de Automática e Informática industrial*, 205-216. doi:10.1016

- González, J., Myer, R., & Pachón, W. (2017). La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo. *Revista Científica General José María Córdov, 15*(19), 269-289. Obtenido de http://www.scielo.org.co/scielo.php?pid=S1900-65862017000100269&script=sci_abstract&tlng=es

- Guevara, C. (2018). *Desarrollo de algoritmos eficientes para identificación de usuarios en accesos informáticos.* Madrid: Universidad Complutense de Madrid. Obtenido de http://eprints.ucm.es/46037/1/T39510.pdf

- López, M. (2017). Hacking ético. Vulnerabilidad de Sistemas Operativos en el acceso por contraseñas. *Revista Publicando, 10*(1), 31-51. Obtenido de

https://www.rmlconsultores.com/revista/index.php/crv/article/viewFile/407/pdf_259

- Martelo, R., Tovar, L., & Maza, D. (2018). Modelo Básico de Seguridad Lógica. Caso de Estudio: el Laboratorio de Redes de la Universidad de Cartagena en Colombia. *Información Tecnológica, 29*(1), 3-10. doi:10.4067
- Muñoz, C. (2002). *Auditoría en Sistemas Computacionales.* México: Editorial Pearson Education.
- Quiroz, S., & Macías, D. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias, 3*(5), 137-156. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=6137824
- Sánchez, A., Fernández, J., Toval, A., Hernández, I., Sánchez, A., & Carrillo, J. (2014). Guía de buenas prácticas de seguridad informática, en el tratamiento de datos de salud para el personal sanitario en atención primaria. *Atención Primaria, 46*(4), 214-222. doi:10.1016
- Santiago, E., & Sánchez, J. (2017). Riesgos de ciberseguridad en las empresas. *Revista de Ciencia, Tecnología y Medio Ambiente*(15), 1-33. Obtenido de https://revistas.uax.es/index.php/tec_des/article/download/1174/964
- Serrato, G. (2016). Metodología para el análisis de vulnerabilidades. *Tecnología, Investigación y Academia, 4*(2), 20-27. Obtenido de https://revistas.udistrital.edu.co/ojs/index.php/tia/article/view/7625/pdf
- Suarez, D., & Ávila, A. (2015). Una forma de interpretar la seguridad informática. *Journal of Engineering anda technology*, 16-23. Obtenido de http://repository.lasallista.edu.co:8080/ojs/index.php/jet/article/view/1015/1072
- Vega, G., & Ramos, R. (2017). Vulnerabilidades y Amenazas a los servicios web de la Intranet de la Universidad Técnica de Babahoyo. *3C Tecnología, 6*(1), 53-66. Obtenido de https://www.3ciencias.com/wp-content/uploads/2017/03/ART5.pdf

ANEXOS

Anexos A: Guía de auditoria

EMPRESA "CUESGAR S.A"				**Fecha:** 17/12/2018 **Hora:** 08:00 a.m.
Referencia	**Actividad a evaluar**	**Procedimientos de auditoría**	**Herramientas utilizadas**	**Observaciones**
AUD - 01	Evaluar las políticas y el manejo del programa contable	• Determinar si existen políticas para el manejo de los programas • Verificar si han sido socializadas las políticas. • Verificación de contraseñas	• Cuestionario • Ficha de observación	-
AUD - 02	Determinar el cumplimiento de las funciones y actividades del personal	• Verificar el cumplimiento de actividades • Conocimiento y destrezas del personal	• Cuestionario	-
AUD - 03	Operaciones físicas y lógicas	• Comprobar si el antivirus se encuentra actualizado • Identificar si el sistema operativo funciona correctamente. • Verificar si se tiene preocupación con los mensajes recibidos en los correos electrónicos.	• Ficha de observación • Cuestionario	-

Anexos B: Matriz de evaluación

Descripción de los conceptos que se evaluaran	**Calificación**				
	10: Excelente	**8: Bueno**	**6: Suficiente**	**4: Regular**	**2: Deficiente**
Políticas y manejos del programa contable					
Socialización de las políticas	La empresa cuenta con políticas, en donde detallan el procedimiento y las medidas de seguridad que deben realizar y las mismas son socializadas constantemente.	Las políticas relacionadas a los procedimientos y medidas de seguridad son socializadas de vez en cuando.	La empresa cuenta con políticas acerca de los procedimientos y medidas de seguridad, pero solo fueron socializadas una vez.	Si existen políticas que definen el procedimiento que deben seguir, pero en lo que respecta a medidas de seguridad no existen.	No existen políticas para el manejo del programa contable.
Documentación de las políticas	Las políticas se encuentran documentadas detallan el proceso, cronología y motivo a seguir dependiendo de la situación que se presente.	Las políticas son documentadas de manera que definen el proceso y motivo a realizar.	Las políticas son documentadas, indicando el motivo a realizar, pero no definen correctamente el proceso a seguir.	Las políticas que poseen, no se encuentran documentadas.	No existen políticas en la empresa.
Verificación de contraseñas	La contraseña para ingresar al programa es de uso exclusivo del trabajador.	La contraseña del trabajador, la sabe también otra persona de la empresa.	La contraseña de ingreso del trabajador, es conocido por dos trabajadores más.	Todas las personas conocen la clave y usuario de ingreso al programa.	Las contraseñas del sistema se encuentran visibles para todas las personas que ingresan a la empresa.

Funciones y actividades del personal					
Cumplimiento de actividades	El personal de la empresa cumple correctamente las actividades asignadas de manera eficiente.	La mayoría de actividades las cumplen correctamente los trabajadores.	El cumplimiento del personal de acuerdo a sus actividades es regular.	El personal de la empresa cumple ineficientemente las actividades.	El personal no cumple con las actividades correspondientes en su trabajo.
Conocimiento y destreza del personal	Los trabajadores cuentan con el conocimiento, experiencia necesaria en informática y en el manejo y seguridad de programas.	Los trabajadores tienen el conocimiento, experiencia y manejo de programas.	El personal posee tres años de experiencia en el manejo de programas contables.	El personal solo cuenta con el conocimiento mínimos de computación.	El personal de la empresa no cuenta con la experiencia ni conocimientos adecuados.
Operaciones físicas y lógicas					
Antivirus	Todas las computadoras tienen antivirus, además se encuentran actualizados y cuentan con licencia.	Las computadoras tienen antivirus actualizados pero no poseen la licencia.	Dos computadoras poseen antivirus actualizados.	Las computadoras cuentan con antivirus, pero no estan actualizados.	Las computadoras no tienen antivirus.
Sistema Operativo	La empresa cuenta con el Sistema Operativo Windows 10 y tiene la licencia correspondiente.	La empresa posee el sistema Windows 10 pero no tiene la licencia.	El sistema operativo que poseen las computadoras es el Windows 8, pero sin licencia.	Poseen otra versión de sistema operativo, pero sin licencia	Poseen el Windows XP las computadoras.

Correos electrónicos	Los correos electrónicos son revisados con cautela, y no se proporciona información confidencial de la empresa.	Se analiza los correos electrónicos, teniendo el cuidado de la información a tratar.	Los correos electrónicos son revisados pero cierta información confidencial se proporciona.	Se tiene poco cuidado al momento de responder correos electrónicos.	Se proporciona información confidencial de la empresa.

Anexos C: Cuestionario de Seguridad Informática a la Empresa "CUESGAR S.A"

Dirigido al personal de la empresa

Punto a evaluar: Políticas y manejos del programa contable

Socialización de las políticas con el personal de la empresa

1. ¿La empresa cuenta con políticas que indiquen los procedimientos de manejo y seguridad que deben realizar los empleados?

☐ **Si**

☐ No

Observaciones:

La empresa si cuenta con políticas, pero se evidencia que poseen pocos controles de seguridad y en lo que respecta a detallar procedimientos se encuentran generalizados.

2. ¿De qué forma son socializadas las políticas con los empleados?

☐ Afiches

☐ Carteles

☐ Correos electrónicos

☐ Otros

Observaciones:

Las políticas son socializadas de vez en cuando con el personal al momento de ingresar nuevos personales, también se envía correos electrónicos a los trabajadores indicando las políticas.

Documentación de las políticas

3. ¿Las políticas son documentadas?

☐ Si

☐ No

Verificación de contraseñas

4. ¿Las contraseñas de ingreso al sistema es de uso exclusivo de la persona encargada?

☐ Si

☐ No

Observaciones:

Todo el personal tiene conocimiento de la clave y usuario para ingresar al sistema contable, lo cual no es recomendable.

Punto a evaluar: Operaciones físicas y lógicas

Antivirus

5. ¿El antivirus que cuentan las computadoras se encuentra actualizado?

☐ Si

☐ No

Observaciones:

Se evidencio que no están actualizados los antivirus.

Sistema Operativo

6. ¿Qué tipo de versión de sistema operativo cuentan en la empresa?

Windows 8

Correos electrónicos

7. ¿Al momento de recibir mensajes en el correo electrónico ingresan informacion confidencial de la empresa?

☐ Si

☐ No

Observaciones:

Se evidencio que no existe control en la recepción de correos y en la mayoría de casos proporcionan información confidencial sin asegurarse de la veracidad del sitio que pide la información.

8. ¿La contraseña del correo electrónico tiene conocimiento todo el personal?

☐ **Si**

☐ No

Dirigido al administrador de la empresa

Punto a evaluar: Funciones y actividades del personal

Cumplimiento de actividades

1. **¿El personal cumple eficientemente con las actividades propuestas por parte de la empresa?**

☐ Si

☐ No

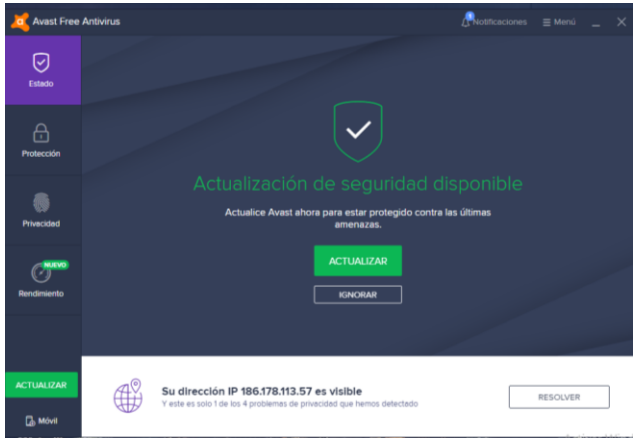
Conocimiento y destreza del personal

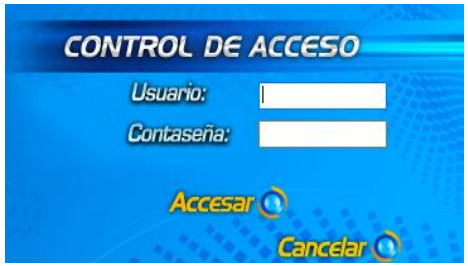
2. **¿El personal de la empresa cuenta con un perfil adecuado para desempeñar las actividades diariamente en la empresa?**

☐ Si

☐ No

Anexos D: Ficha de Observación

<table>
<tr><th colspan="4">FICHA DE OBSERVACIÓN</th></tr>
<tr><td>Ficha</td><td colspan="3">1</td></tr>
<tr><td>Lugar</td><td colspan="3">Empresa “CUESGAR S.A”</td></tr>
<tr><td>Fecha:</td><td colspan="3">Lunes 17 de Diciembre del 2018</td></tr>
<tr><td>Situación:</td><td colspan="3">Ineficiencias en los antivirus</td></tr>
<tr><td>Elaborado por:</td><td colspan="3">Cristhian Neira</td></tr>
<tr><td>Tipo de Observación</td><td>Observación</td><td>Detalle</td><td>Evidencia</td></tr>
<tr><td>Seguridad lógica</td><td>En la ejecución de la auditoría se evidencio ineficiencias que presenta el antivirus en las computadoras.</td><td>Las 4 computadoras que cuenta la Empresa “CUESGAR S.A” poseen desactualizaciones en lo que corresponde al antivirus Avast, lo cual ocasiona que el funcionamiento de las computadoras sea lento y propicio para adquirir virus que pongan en riesgo la información de la entidad.</td><td> 
</td></tr>
</table>

FICHA DE OBSERVACIÓN			
Ficha	2		
Lugar	Empresa “CUESGAR S.A”		
Fecha:	Lunes 17 de Diciembre del 2018		
Situación:	Conocimiento de usuario y clave entre trabajadores		
Elaborado por:	Cristhian Neira		
Tipo de Observación	**Observación**	**Detalle**	**Evidencia**
Seguridad lógica	Los empleados conocen el usuario y clave de los diferentes personas que ingresan al sistema contable.	Se evidencio que los trabajadores de la Empresa “CUESGAR S.A” tienen el conocimiento de claves y usuarios de las diferentes personas que ingresan al sistema, lo cual no es recomendable debido a que se puede alterar la información contable y no se podrá definir exactamente quien fue el responsable de dicha acción.	

Anexos E: Matriz de resultados

Descripción de los conceptos que se evaluaran	**Calificación**				
	10: Excelente	**8: Bueno**	**6: Suficiente**	**4: Regular**	**2: Deficiente**
Políticas y manejos del programa contable					
Socialización de las políticas				X	
Documentación de las políticas			X		
Verificación de contraseñas				X	
Funciones y actividades del personal					
Cumplimiento de actividades			X		
Conocimiento y destreza del personal			X		
Operaciones físicas y lógicas					
Antivirus				X	
Sistema Operativo			X		
Correos electrónicos				X	

Anexos F: Matriz de Riesgo

No.	Factores de riesgo	Impacto			Probabilidad			Niveles de riesgos	Control existente	Departamento		Dirección	
		A	M	B	A	M	B			Causas	Consideraciones	Cronograma	Responsable
1	Políticas para el manejo y seguridad de la información son generalizadas y pocas socializadas con el personal.	X				X		Alto	Las políticas solo son socializadas al ingreso de nuevo personal y no detallan correctamente los pasos a seguir	No prestan la atención adecuada al desarrollo de políticas eficientes.	Realizar políticas que definan correctamente los procesos a seguir y que las políticas sean socializadas constantemente para asegurar el funcionamiento en la empresa.	Permanente	Administrador
2	Conocimiento entre trabajadores de las claves para el ingreso	X			X			Alto	Ninguno	Socialización entre empleados de contraseñas de ingreso al sistema.	Establecer una política en que mencione que no deben dar su contraseña a otro usuario.	Permanente	Administrador

3	Antivirus desactualizados en las computadoras	X			X			Alto	Ninguno	No se presta la atención suficiente a la protección de virus.	Contar con antivirus actualizados constantemente para salvaguardar la información.	Permanente	Administrador
4	En los correos electrónicos se puede incurrir en dar información confidencial	X				X		Medio	Ninguno	No conocen los riesgos que pueden ocurrir, al momento de proporcionar información confidencial de la empresa	Tener cuidado con la información que es solicitada por correo electrónico.	Permanente	Todos los trabajadores