UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

# AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA COMPUTRONIC S.A DE LA CIUDAD DE EL GUABO

ANGULO VERA DOUGLAS LEONARDO
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

# AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA COMPUTRONIC S.A DE LA CIUDAD DE EL GUABO

ANGULO VERA DOUGLAS LEONARDO
INGENIERO EN CONTABILIDAD Y AUDITORÍA CPA

MACHALA
2019

# UTMACH

## UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

## CARRERA DE CONTABILIDAD Y AUDITORÍA

EXAMEN COMPLEXIVO

# AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA COMPUTRONIC S.A DE LA CIUDAD DE EL GUABO

ANGULO VERA DOUGLAS LEONARDO
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 AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA COMPUTRONIC S.A DE LA CIUDAD DE EL GUABO, 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 - 09:47

# Urkund Analysis Result

| | |
|---|---|
| **Analysed Document:** | ANGULO VERA DOUGLAS LEONARDO_PT-011018.pdf (D47177810) |
| **Submitted:** | 1/24/2019 12:46:00 AM |
| **Submitted By:** | titulacion_sv1@utmachala.edu.ec |
| **Significance:** | 2 % |

## Sources included in the report:

https://www.monografias.com/docs113/modelo-auditoria-seguridad-informatica-red-datos/modelo-auditoria-seguridad-informatica-red-datos.shtml
http://polux.unipiloto.edu.co:8080/00003023.pdf

## Instances where selected sources appear:

3

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

El que suscribe, ANGULO VERA DOUGLAS LEONARDO, en calidad de autor del siguiente trabajo escrito titulado AUDITORIA DE SEGURIDAD INFORMÁTICA A LA EMPRESA COMPUTRONIC S.A DE LA CIUDAD DE EL GUABO, 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

Angulo Vera Douglas

ANGULO VERA DOUGLAS LEONARDO
1003977855

## DEDICATORIA

El presente trabajo investigativo lo dedicamos principalmente a Dios, por ser el inspirador y darme fuerza para obtener uno de los anhelos más deseados.

A mis padres, por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes he logrado llegar hasta aquí y convertirme en lo que soy ahora. Ha sido el orgullo y el privilegio de ser su hijo, son los mejores padres.

A mis hermanos por estar siempre presentes, acompañándome y por el apoyo moral, que me brindaron a lo largo de esta etapa de mi vida.

A todas las personas que me apoyaron y han hecho que el trabajo se realice con éxito en especial a aquellos que me abrieron las puertas y compartieron sus conocimientos.

***Douglas Leonardo Angulo Vera***

## AGRADECIMIENTO

Agradezco a Dios por derramar sus bendiciones en mi vida, a lo largo de mi preparación académica y profesional, ser el apoyo y fortaleza en aquellos momentos de dificultad y de debilidad.

Gracias a mis padres: Amanda Vera Robinzon y José Angulo González por ser los principales promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado.

Agradecemos a nuestros docentes de la Carrera de Contabilidad y Auditoría de la Universidad Técnica de Machala, por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión, de manera especial, a la Ingeniera Ordoñez Briceño Karla Fernanda docente y tutora del caso práctico de tesis, quien ha guiado con paciencia, y rectitud como docente.

***Douglas Leonardo Angulo Vera***

## RESUMEN

En el presente trabajo, la auditoría de la seguridad informática, se elaboró con el propósito de hacer una auditoría a la empresa Computronic S.A donde el caso a presentar es un modelo lógico para dirigir la auditoría de seguridad informática, definiendo los niveles de seguridad existentes y la forma en que los riesgos son disminuidos. Esta auditoría tiene como fin detectar amenazas y vulnerabilidades en el hardware y software, con el fin de obtener información segura de sus activos y as para precautelar la información informática que cuenta la organización ya que no es suficiente con escribir un manual de seguridad, instalar las mejores herramientas y tener la mejor capacitación del personal, sino más bien de auditar de manera correcta, aplicando mecanismos de seguridad utilizados en el ofrecimiento de los servicios de tecnologías de información. Ya que por ello, es muy importante aplicar los controles de seguridad informática. El término auditar correctamente incluye varios elementos importantes, uno de ellos es contar con un modelo de auditoría completo, equilibrado y técnicamente correcto. Este trabajo propone un modelo de auditoría de la seguridad informática para aquellos servicios que se ofrece para a la entidad antes mencionada. Así mismo se indican que los resultados alcanzados dentro de la elaboración de la auditoría informática, se han podido evidenciar hallazgos y en base a esto se pudo realizar las respectivas recomendación, con el fin de determinar la eficacia y eficiencia de los recursos informáticos, para que así la empresa lleve sus actividades laborales de manera óptima.



**Palabras claves:** Seguridad Física y lógica, Auditoría informática, Recursos informáticos.

## ABSTRACT

In the present work, the audit of computer security, the same step for the purpose of making an audit the company Computronic SA where the case is a logical model to manage the computer security audit, defining the current security levels and the way in which the risks are diminished. This audit aims to identify and vulnerabilities in the hardware and software, in order to obtain secure information of their assets and as a precaution in the computer information that the organization has and that is not enough with a security manual, install the best tools and have the best staff training, but rather in a correct way, applying the security mechanisms in offering the services of information technologies. That is why it is very important to apply computer security controls. The term auditing correctly includes several important elements, one of them is to have a complete, balanced and technically correct audit model. This paper proposes a computer security audit model for those services offered for the aforementioned entity. Likewise, you can see the results achieved within the development of the computer audit, it has been possible to show findings and based on this you can make the respective recommendations, in order to assess the effectiveness and efficiency of computing resources, So that, the company can carry out its work activities optimally.



**Keywords**: Physical and logical security, computer audit, computer resources.

**ÍNDICE**

## ÍNDICE DE TABLAS

# INTRODUCCIÓN

La seguridad informática, es hoy día uno de los factores importantes en la empresa. Por lo que se ha convertido cada vez más en una necesidad irremediable y urgente para todos, ya que con la auditoría se podrá contar con manuales de análisis, y control de debilidades, para así analizar los riesgos más comunes en el sistema informático en el área de ventas de la empresa. Cabe aclarar que la auditoría informática ayuda a la toma de decisiones, debido a esto la organización mejora sus acciones con la finalidad de llevar a cabo los procedimientos, normas y políticas establecidos.

La palabra auditoría ha sido colocada erróneamente con continuidad, ya que se ha estimado como una valoración con el fin de mitigar errores y fallas. La seguridad informática evalúa los controles de seguridad, cuyo fin es detectar errores mediante un informe detallado de las vulnerabilidades, problemas, fallos que se hayan encontrado, y así se aplique los respectivos procedimientos para mitigar los riesgos, donde estos resultados es entregado al responsable de los controles del centro de cómputo evaluado, con el objetivo de realizar de informar los hallazgos encontrados para así salvaguardar los activos de la empresa.

En el presente trabajo se pretende desarrollar una auditoría de planeación, ejecución y dictamen, basado a la metodología del autor Muñoz, (2002) con el fin de llevar de una manera adecuada sus actividades en la entidad, para así eliminar las disfunciones y debilidades antedichas, estas sugerencias también pueden estar plasmadas en el informe final , la cual reciben el nombre de recomendaciones, para que sea de ayuda en la auditoría del sistema informático de la empresa Computronic S.A de la ciudad del Guabo.

# 1. FUNDAMENTACIÓN TEÓRICA

## 1.1 Auditoría Interna

Es un proceso que analiza las cuentas con el fin de tener una imagen razonable fiel dentro de la sociedad lo que el Autor Rodríguez (2012) comenta también que: “la auditoría es considerada como proceso informacionales.” (pág. 3). Ya que por ende puede tomar la información con el fin de asegurar que se han registrado y reflejado lo presentado por las entidades la cual ayude al crecimiento de las entidades, generando mejoras de información.

La auditoría aparte de descubrir un fraude, realiza análisis de la información para que en el transcurso del trabajo se pueda evidenciar su situación patrimonial y económica por lo que los autores Salas y Ponjuán (2014) nos manifiesta que también se debe hacer una “auditoría de conocimiento como parte de enfoques estratégicos.” (pág. 2) la cual se encarga de verificar y analizar si se está cumpliendo adecuadamente las normas y políticas de la organización.

## 1.2 Control Interno

Es una auditoría interna, es decir, lo hacen las personas de la misma institución para detectar robos, fraudes, conflictos dentro de la organización, en este sentido Vega de la Cruz y González (2017) manifiesta que “las organizaciones deben lograr un eficiente control interno” (pág. 3) para así tener un crecimiento en la entidad, que ayuden a mejorar tanto normas, políticas, métodos y procedimientos para valorar la exactitud de la validez de su información.

El control interno es de vital importancia, ya que ayuda a reducir los riesgos de corrupción, lograr objetivos y metas establecidas, promover el desarrollo organizacional, por ende los autores, Gómez, Estrada, René, y García (2012) comentan que: “se debe evaluar el cumplimiento de normativas” (pág. 5) que ayude al proceso de contar información confiable y oportuna que permite detener los problemas antes de su operación y así asegurar información verídica que ayuda a los empresarios a realizar de manera adecuada y oportuna sus actividades laborales.

### 1.3 Auditoría Informática

Es la revisión y evaluación de controles, sistemas y procedimientos de los equipos informáticos para la utilización del procesamiento de información la cual es de vital importancia ya que se investiga todo y cada uno de los aspectos importantes relacionado con dispositivos informáticos, el autor, Rodríguez (2012) comenta que también ayuda a la auditoría informática: “la auditoría de información y la auditoría de conocimiento” (pág. 5). Ya que permite hacer una investigación y conocer el estado de la entidad organizacional, examinar recursos de conocimiento, que se adquiere y usan en la entidad para realizar sus actividades cotidianas empresariales.

### 1.4 Seguridad Informática

Es el proceso de informar y revelar el uso no considerado de los sistema informáticos la cual esta se encargara de proteger y transmitir toda la información digital de manera segura, los autores Gil y Gil (2017) manifiesta que: **“**La seguridad de la información tiene por objeto proteger a los sistemas informáticos” (pág. 194) la cual abarca una serie de medidas de seguridad, como programas de software de antivirus, firewall y otras medidas que ayude a mitigar pérdidas tanto monetarias como físicas para la empresa.

La seguridad informática consiste en asegurar que los recursos del sistema de información de una organización sea utilizada bajo la supervisión del gerente o de la persona a cargo. Los autores Díaz, Pérez, y Proenza (2014) también señalan que la auditoría informática es un: “importante número de disciplinas y especialidades distintas y complementarias” (pág. 2) que implica al proceso de proteger contra intrusos al sistema informático con intenciones de obtener ganancias, por ende se pretende salvaguardar información mediante políticas que ayuden a las entidades a tener seguridad.

### 1.5 Delitos Informáticos

Los delitos informáticos son todas aquellas conductas ilícitas susceptibles de ser sancionadas, que hacen un uso indebido de cualquier medio informático. El autor Contreras (2006) comenta que los delitos informáticos: “atentan contra diversos bienes jurídicos, a saber, la propiedad, la intimidad.” (pág. 516). De la entidad la cual este podría generar pérdidas de la información empresarial como también pérdidas económicas.

Los delitos informáticos lo consiguen mediante el uso de computadoras, u otros aparatos que genera una operación ilícita que se realiza a través de un medio informático, este medio puede ser hardware o software o la combinación de ambos, la autora Mayer (2017) afirma que los delitos informáticos también son conocidos también como: “criminalidad informática en sentido amplio o criminalidad cometida” (pág. 245). Los mismos que son usados de manera inadecuada, por ello las empresas optan por tener un mejor respaldo de seguridad informática que ayuden a mitigar los delitos informáticos.

### 1.6 Políticas de Seguridad Informática

Son reglas que usan las organizaciones para salvaguardar la información de la empresa, para ello debe definir claramente sus objetivos de seguridad y así crear reglas y procedimientos que cada usuario debe seguir, la autora López (2015) plantea que las políticas deben ser: “Cuidados de larga duración” (pág. 2)” ya que en estas normas la empresa puede basarse en estándares internacionales que marcan la forma en la que se debe manejar la información en la empresa.

# 2. DESARROLLO

## 2.1 Metodología

La metodología aplicar es deductivo e inductivo de Muñoz (2002) que trata de analizar los datos obtenidos y proporcionados por la entidad para así tener una mejora continua y proceder a las respectivas toma de decisiones que ayude a mitigar los riesgos en la empresa Computronic S.A de la ciudad del Guabo.

- Planeación
- Ejecución
- Dictamen

### *2.1.1 Fase de Planeación*

#### *2.1.1.1 Origen de la Auditoria***.**

La auditoría se la va a realizar en la empresa Computronic S.A. de la ciudad de el Guabo, ya que cuenta con un escaso rendimiento de seguridad informática, por consiguiente se procede a realizar una auditoría informática para mejorar las actividades laborales de la empresa.

**DATOS DE LA EMPRESA**

**RAZÓN SOCIAL**

Computronic S.A

**REGISTRO ÚNICO DE CONTRIBUYENTES**

0703686667001

**FECHA DE CONSTITUCIÓN**

Computronic  S.A se constituyó en el cantón de Santa Rosa el 01 de septiembre del 2014.

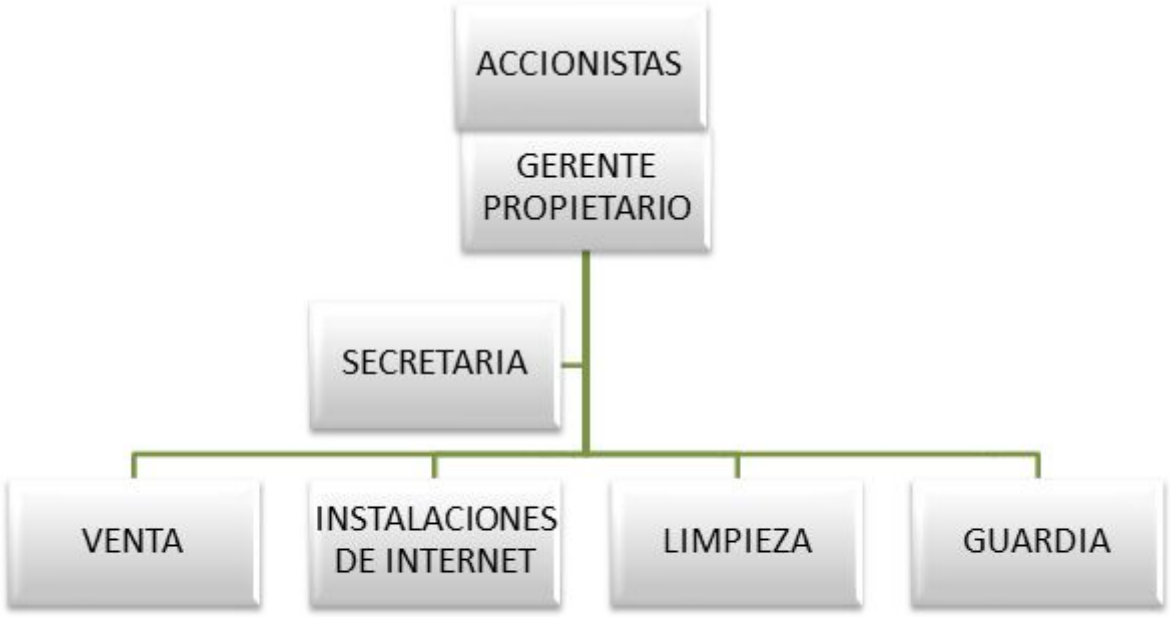
**ACTIVIDAD PRINCIPAL**

Computronic S.A tiene como actividad principal dedicarse a la venta de internet.

**DIRECCIÓN**

Sucre y Machala

**ORGANIGRAMA**




**Fuente:** Computronic S.A

**Elaborado por:** Douglas Leonardo Angulo Vera.

### *2.1.1.2 Visita Preliminar*

El martes 5 de diciembre del 2017 a las 9:30 am, el equipo auditor realiza una visita preliminar a la empresa a auditar, donde se pudo evidenciar un bajo rendimiento en los equipos informáticos que usa el área de ventas. En esta visita obtuvimos información del hardware y software que maneja este departamento.

### *2.1.1.3 Objetivo de la Auditoría*

La empresa Computronic S.A no cuenta con un programa de auditoría, por lo que le sería de vital importancia para la entidad encontrar deficiencias ya sea en los procesos que siguen o en el equipo que manejan.

#### *2.1.1.3.1 Objetivos Específicos*

- Revisar la suficiencia de los controles que existen en esa área.
- Analizar los riesgos más comunes en el sistema informático en el área de ventas.
- Verificar el cumplimiento de los controles.
- Realizar entrevista con la persona encargada del área de venta, utilizando como herramienta un cuestionario con los diferentes temas a evaluar, para tener información.
- Tomar evidencias con fotografía del medio de trabajo del área de ventas y sus equipos para mostrar resultado de lo que se podría mejorar.
- Analizar los riesgos más comunes en el área de ventas.

**Seguridad Física**

- Verificar la actualización del hardware
- Verificar controles de accesos físicos al centro de computo
- Mantenimiento preventivo y correctivo

**Seguridad Lógica**

- Verificar la actualización del software, antivirus, paquetes office.
- Protección y respaldo de información.
- Existencia de políticas de seguridad de la información.
- Verificar restricción de acceso sitios web no permitidos.
- Personal
- Verificar títulos, capacitaciones y experiencia laboral.

*2.1.1.4 Puntos a Evaluar*

**Seguridad Física**

- Revisar si cuenta con actualizaciones del hardware.
- Revisar si la entidad cuenta con controles de accesos físico al centro de cómputo.
- Revisar si cuenta con mantenimiento preventivo y detectivos.

**Seguridad Lógica**

- Revisar si cuenta con actualización del software.
- Revisar si cuenta con respaldo de información.
- Revisar si cuenta con políticas de seguridad de la información.
- Revisar si tiene restricción de acceso sitios web no permitidos.

**Personal**

- Revisar si los empleados cuenta con títulos, capacitaciones y experiencia laboral.

## 2.2. Guía de Auditoría

**Tabla 1. Guia de Auditoria**

| REF | ACTIVIDADES QUE SERA EVALUADA | PROCEDIMIENTO DE AUDITORIAS | HERRAMIENTAS QUE SERAN UTILIZADAS | OBSERVACIÓN |
|---|---|---|---|---|
| | | Seguridad Física | | |
| | Verificar la actualización del hardware | 1.- Equipos alternos en caso de fallos en el uso de ellos. | Experimentación | Documentar los accesos y cambios que se al momento de hacer cambio a las computadoras. |
| | Verificar controles de accesos físico al centro de computo | 1.- Solicitar al encargado del área la lista de equipos que se usan, cuantos usuarios las usan y cuantas horas al día son usados estos equipos. | Revisión documental | Llevar previamente elaborado el cuestionario de las entrevistas y los cuestionarios de las encuestas. |
| | Mantenimiento preventivo y correctivo | 1.- Revisar mediante la elaboración de una actividad si los equipos informáticos dan con los resultados esperados por la empresa. | | El sistema por ningún medio debe permitir el acceso sin contraseña y al tercer intento bloquear la terminal. |
| | ➢ Se procede a la revisión de los equipos para el uso de la empresa. | | | |
| | ➢ Evaluar d que los equipos informáticos responden de acuerdo al uso del usuario. | | | |

Elaborado por: El Autor

| Seguridad Lógica | | | |
|---|---|---|---|
| **Minimizar los riesgos de perdida de información por fallos de los equipos computacionales** | 1.- Respaldo de información crítica y antivirus. | Observación. | Guardar información y archivarla y contar con antivirus para que no afecte a la información de la organización. |
| **Verificar la actualización del software, antivirus, paquetes office.** | 1.-Revisar que los equipos informáticos cuenten con antivirus y sus respectivos paquetes office. | Observación. | Tener licencias de antivirus y disco de respaldo de paquete office. |
| **Protección y respaldo de información** | 1.- Plan de contingencia | Encuesta. | Obtener respaldo previo del sistema y los movimientos previos a la prueba. |
| **Existencia de políticas de seguridad de la información** | 1.- Verificar que la empresa cuente con políticas de seguridad. | Revisión. | Contar con políticas de seguridad de la información tanto físicas como en internet. |
| **Verificar restricción de acceso sitios web no permitidos** | 1.-Verificar si los equipos informáticos tienen acceso a las paginas web | Revisión. | Restringir páginas que los empleados no puedan acceder para no dar un uso indebido a sus actividades laboral. |
| ➢ **Se procede a la verificación de información, antivirus, respaldo, políticas y sitios web no permitidos para la empresa.** | | | |

Elaborado por: El Autor

| Personal | | | |
|---|---|---|---|
| Verificar títulos y capacitaciones y experiencia laboral | 1.- Comprobar que la empresa cuente con personal profesional para solicitar el cargo. | Experimentación. | Verificar que los trabajadores tengan título profesional y experiencia laboral. |
| ➢ **Se procede a verificar si la empresa cuenta con personal profesional, para ejercer el cargo.** | | | |

Elaborado por: El autor.

*2.2.1 Matriz de Evaluación*

**Tabla 2. Matriz de Evaluación**

| Punto a evaluar | 10<br>Excelente | 9<br>Suficiente | 8<br>Deficiente |
|---|---|---|---|
| Verificar la actualización del hardware | El auditor investigo a fondo con total cautela, seguridad y con excelente disposición si los sistemas informáticos cumple con actualizaciones del hardware. | El auditor investigó con la suficiente profundidad si los equipos informáticos cumplen con actualizaciones de hardware. | El auditor investigó sin la mínima profundidad si los equipos informáticos cumplen con actualizaciones de hardware. |
| Verificar si los equipos que se utiliza cumple con los requisitos establecidos | El auditor investigo a fondo con total cautela, seguridad y con excelente disposición si los sistemas informáticos cumple con los requisitos establecidos por el cliente. | El auditor investigó con la suficiente profundidad si los equipos informáticos cumplen con los requisitos establecidos por el cliente. | El auditor investigó sin la mínima profundidad si los equipos informáticos cumplen con los requisitos establecidos por el cliente. |
| Mantenimiento preventivo y correctivo | El auditor investigó a fondo con total cautela, seguridad y con excelente disposición si dan mantenimiento preventivo y correctivo | El auditor investigo con la suficiente profundidad las existencias de mantenimiento preventivo y correctivo. | El auditor investigó sin la mínima profundidad las existencias de mantenimiento preventivo y correctivo. |
| Minimizar los riesgos de perdida de información por fallos de los equipos computacionales | El auditor investigo a fondo con total cautela, seguridad y con excelente disposición la existencias de minimizar riesgos de perdida de información por fallos de los equipos computacionales. | El auditor investigó con la suficiente profundidad las existencias de minimizar riesgos de perdida de información por fallos de los equipos computacionales. | El auditor investigó sin la mínima profundidad por lo tanto no sabe minimizar riesgos de perdida de información por fallos de los equipos computacionales. |

| | | | |
|---|---|---|---|
| Verificar la actualización del software, antivirus y paquetes office | El auditor investigó a fondo con total cautela, seguridad y con excelente disposición la existencia de actualizaciones del software, antivirus y paquetes office. | El auditor investigó con la suficiente profundidad las existencias de actualizaciones del software, antivirus y paquetes office. | El auditor investigó sin la mínima profundidad por lo tanto no sabe las existencias de actualizaciones del software, antivirus y paquetes office. |
| Protección y respaldo de información computacionales | El auditor investigó a fondo con total cautela, seguridad y con excelente disposición si cuenta con protección y respaldo de información computacionales. | El auditor investigó con la suficiente profundidad si cuenta con planes de protección y respaldo de información computacionales. | El auditor investigó sin la mínima profundidad por lo tanto no sabe si cuenta con planes de protección y respaldo de información computacionales. |
| Existencia de políticas de seguridad de la información | El auditor investigó a fondo con total cautela, seguridad y con excelente disposición si cuenta con políticas de seguridad de la información. | El auditor investigó con la suficiente profundidad si cuenta con políticas de seguridad de la información. | El auditor investigó sin la mínima profundidad por lo tanto no sabe si cuenta con políticas de seguridad de la información |
| Verificar restricción de acceso sitios web no permitidos | El auditor investigó a fondo con total cautela, seguridad y con excelente disposición si cuenta con restricción de acceso sitios web no permitidos. | El auditor investigó con la suficiente profundidad si cuenta con restricción de acceso sitios web no permitidos. | El auditor investigó sin la mínima profundidad por lo tanto no sabe si cuenta con restricción de acceso sitios web no permitidos. |

Elaborado por: El Autor

## 3. CONCLUSIÓN

### 3.1 Dictamen de la Auditoría

**Tabla 3. Dictamen**

Auditorías Soluciones S. A.
Auditores y consultores gerenciales

SITUACIONES ENCONTRADAS

**EMPRESA AUDITADA:** COMPUTRONIC S.A. AREA AUDITADA: **VENTAS**

FECHA: **27/12/2017**

| REF. | SITUACIONES | CAUSAS | SOLUCION | FECHA DE SOLUCION | RESPONSABLE |
|---|---|---|---|---|---|
| **S001** | Computadora obsoleta | • Falta de presupuesto.<br>• Falta de organización. | Colocar en el presupuesto de la entidad la compra de una computadora actual que cumpla con las características para el buen funcionamiento de las actividades empresariales. | 07/01/2019 | Junta directiva |
| **S002** | Falta de instructivo o manual para el uso de los equipos informáticos. | • No existen un instructivo ni un manual. | Implementación de un instructivo o un manual | 08/01/2019 | Gerente propietario |
| **S003** | Falta de mantenimiento a los equipos informáticos. | • Errores en los equipos informáticos. | Darles un mantenimiento constante a los equipos informáticos. | 11/01/2019 | Técnico informático |
| **S004** | Reporte de cambios realizados en los equipos informáticos. | • No contar con un respaldo de seguimiento de los cambios de los equipos informáticos. | Llevar un seguimiento de cada vez que se le realiza cambios de los equipos informáticos. | 18/01/2019 | Técnico informático |
| **S005** | Falta de políticas de seguridad. | • No existen política de seguridad ni de responsabilidad para cada | Implementación de políticas donde se establezcan responsabilidades para cada | 14/01/2019 | Junta directiva<br>Contador |
| **S006** | Claves inapropiadas. | • La clave es de uso general para todo el personal.<br>• Todas las aplicaciones y correo tienen la misma clave. | Establecer claves personalizadas según la relevancia o importancia de información. | 15/01/2019 | Junta directiva |
| **S007** | Falta de provisión de energía eléctrica. | • Falta de recursos.<br>• No existe una planta de energía. | Adquirir un regulador o/y planta de energía que proporcione mayor seguridad del hardware. | 16/01/2019 | Junta directiva |
| **S008** | Acceso libre a páginas web. | • No existen bloqueos de ciertos sitios webs. | Bloquear páginas no destinadas a las labores como: Facebook, Instagram o twitter. | 17/01/2019 | Técnico informático |

Elaborado por: El Autor

### *3.1.1 Situaciones Detectadas*

**Hallazgos de la Auditoría**

- **Equipos informáticos sin mantenimiento**

Pudimos entender de acuerdo con la versión por parte de la encargada del departamento de venta que no le han realizado monitoreo ni revisión a los equipos informáticos.
La causa de esto es que debido al desconocimiento que tiene el encargado de sistema sobre los periodos que deben de darle un mantenimiento a los equipos informáticos, por tanto, el efecto es que equipos pueden dejar de funcionar en cualquier momento menos pensado, ya que puede sufrir un colapso en cualquier momento.

### *3.1.2 Conclusión*

- En la actualidad en informática es muy importante para el adecuado desempeño de los sistemas de información, debido a que nos brinda los sistemas de información, debido a que nos brinda los controles suficientes y necesarios para que los sistemas sean de alta confiabilidad y con alto nivel de seguridad. Además este tipo de auditorías debe evaluar todo el sistema de información.

- Con este tema, la primordial conclusión a la que se llega, es que toda empresa, que posea sistema de información mediante complejos, debe ser sometida a un control detallado con una evaluación eficiente y eficaz. En la actualidad más del noventa por ciento de las empresa cuentan con su información de forma estructurada a los sistemas informáticos, causa por la que es de vital importancia que los sistemas de los sistemas de información deben funcionar correctamente.

- Cabe mencionar que el éxito de cualquier empresa, siempre dependerá de la eficiencia de sus sistemas de información, es por tal motivo que la auditoría a estos sistemas debe ser realizada de manera correcta.

## BIBLIOGRAFÍA


Contreras, A. (2006). DELITOS INFORMÁTICOS: UN IMPORTANTE PRECEDENTE. (Editorial Universidad de Talca, Ed.) Ius et Praxis, 515-521.

Díaz, R., Pérez, d., & Proenza, P. (2014). Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias. Ciencias Holguín, 20(2), 1-14.

Finquelievich, S. (2010). ARTÍCULOS. Revista iberoamericana de ciencia tecnología y sociedad, 5(15), 2-10.

Gil, V., & Gil, J. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de. Scientia Et Technica, 22(2), 193-197.

Gómez, O., Estrada, V., René, B., & García, I. (2012). Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones. ACIMED, 23(2), 2-10.

Mayer, L. (2017). EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS. Revista Chilena de Derecho, 44(1), 235-260.

Rodríguez, Y. (2012). Auditoría de información y conocimiento en la organización. Ingeniería Industrial, 33(3), 3.

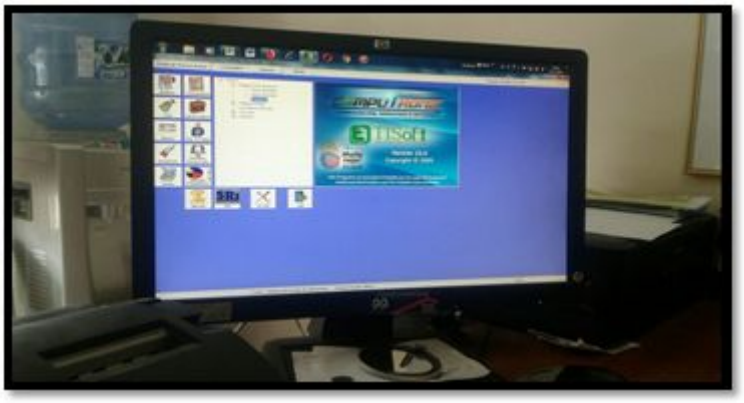
Rodríguez, Y. (2012). Auditoría de información y conocimiento en la organización. Ingeniería Industrial, 33(3).

Salas , G., & Ponjuán, G. (2014). Auditoría del conocimiento orientada a procesos principales en un área biomédica. Revista Cubana de Información en Ciencias de la Salud, 25(3), 1-5.

Vega de la Cruz, L., & Gonzáles, L. (abril de 2017). Diagnóstico estadístico del control interno en una institución hospitalaria. Revista Habanera de Ciencias Médicas, 16(2), 2-4.

## ANEXOS

### Anexo 1. Verificación del Equipo Informático



### Anexo 2. Verificar Funcionamiento del Equipo Informático