



# UTMACH

UNIDAD ACADÉMICA DE CIENCIAS EMPRESARIALES

CARRERA DE CONTABILIDAD Y AUDITORÍA

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA EMPRESA DISROJA  
CÍA. LTDA. EN EL PERIODO 2018.

PESANTES MORA MIGUEL ANGEL  
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  
DISROJA CÍA. LTDA. EN EL PERIODO 2018.

PESANTES MORA MIGUEL ANGEL  
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 DISROJA CÍA.  
LTDA. EN EL PERIODO 2018.

PESANTES MORA MIGUEL ANGEL  
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 DISROJA Cía. Ltda. en el periodo 2018., 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: domingo 03 de febrero de 2019 - 00:30

## Urkund Analysis Result

**Analysed Document:** PESANTES MORA MIGUEL ANGEL\_PT-011018.pdf (D47001903)  
**Submitted:** 1/19/2019 2:53:00 AM  
**Submitted By:** titulacion\_sv1@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, PESANTES MORA MIGUEL ANGEL, en calidad de autor del siguiente trabajo escrito titulado Auditoría de seguridad Informática a la Empresa DISROJA Cía. Ltda. en el periodo 2018., 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.

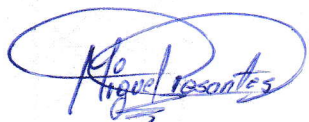
El autor declara que el contenido que se publicará es de carácter académico y se enmarca en las disposiciones definidas por la Universidad Técnica de Machala.

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



PESANTES MORA MIGUEL ANGEL  
0705427136

Auditoría de Seguridad Informática a la Empresa DISROJA Cía. Ltda. En el periodo 2018.

*Autor: Miguel Ángel Pesantes Mora*

*Tutora: Ing. Karla Ordoñez Briceño*

### **Resumen**

El presente trabajo de investigación se refiere a la seguridad informática en la empresa DISROJA Cía. Ltda. Cuyo objeto es de prevenir la fuga de información y evitar que la competencia tenga acceso a su base de datos; si bien es cierto, en la actualidad la tecnología y la globalización está en constante desarrollo, para ello, es necesario estar en alerta de los distintos cambios que pueden afectar el mercado bursátil. Es de gran relevancia que las empresas tengan una buena seguridad informática ya que les permite salvaguardar sus recursos informáticos y contrarrestar los riesgos que pueden restringir su desempeño, por medio este caso se describe las causas y efectos por la que se dio la fuga de información y a su vez proponer medidas de soluciones y recomendaciones ya que son bienes controlados por la empresa lo cual debe ser planificada y contingente. Sin embargo, la vulnerabilidad informática respecto a las amenazas y riesgos en la base de datos está considerado como el caso común que se dan en el mundo de negocio. Desde otra perspectiva, la automatización de los Software tiene como finalidad administrar y controlar la complejidad de los sistemas informáticos. En consecuencia, la ejecución de una auditoría Informática conlleva a implementar diferentes metodologías, técnicas y condiciones notables para su debido proceso como es la planeación, ejecución y el dictamen final, lo cual ayudará a fortalecer la seguridad informática de las entidades Financieras y también señalar cuáles son los factores que conllevan la fuga de Información.

### **Palabras Claves.**

Seguridad Informática, Auditoría Informática, Recursos Informáticos, Sistema de Información, Riesgos Informáticos.

Auditoría de Seguridad Informática a la Empresa DISROJA Cía. Ltda. En el periodo  
2018.

*Autor: Miguel Angel Pesantes Mora*

*Tutor: Ing. Karla Ordoñez Briceño*

### **Summary.**

This research work refers to computer security in the company DISROJA Cía. Ltda. whose purpose is to prevent the leakage of information and prevent competition from having access to its database; although it is true, at present technology and globalization is in constant development, for this, it is necessary to be alert of the different changes that can affect the stock market. It is of great relevance to companies to have a good computer security as it allows them to safeguard their computing resources and counteract the risks that may restrict their performance, through this case, the causes and effects of the information leakage are described and in turn propose measures of solutions and recommendations since they are goods controlled by the company, which must be planned and contingent. However, computer vulnerability regarding threats and risks in the database is considered as the common case in the business world. From another perspective, the automation of the Software is intended to manage and control the complexity of computer systems. Consequently, the execution of an IT audit entails the implementation of different methodologies, techniques and notable conditions for its due process, such as planning, execution and the final opinion, which will help strengthen the IT security of financial entities and also indicate which are the factors that lead to the leakage of information.

### **Keywords**

Computer Security, Computer Audit, Computer Resources, Information System, Computer Risks.



## INDICE

|          |                               |           |
|----------|-------------------------------|-----------|
| <b>1</b> | <b>FUNDAMENTACIÓN TEÓRICA</b> | <b>5</b>  |
| 1.1      | Auditoria                     | 5         |
| 1.2      | Auditoria Informática         | 5         |
| 1.3      | Seguridad informática         | 6         |
| 1.4      | Tecnología Informática        | 6         |
| 1.5      | Vulnerabilidad                | 6         |
| 1.6      | Fuga de Información           | 6         |
| 1.7      | Usuario                       | 6         |
| 1.8      | ISO 27001                     | 6         |
| <b>2</b> | <b>FASE DE LA PLANEACIÓN</b>  | <b>7</b>  |
| 2.1      | Vista Preliminar              | 7         |
| 2.2      | Punto A Evaluar               | 7         |
| 2.3      | Seguridad Física              | 7         |
| 2.4      | Seguridad Lógica              | 8         |
| 2.5      | Seguridad Personal            | 8         |
| <b>3</b> | <b>GUÍA DE AUDITORIA</b>      | <b>8</b>  |
| <b>4</b> | <b>MATRIZ DE EVALUACIÓN</b>   | <b>9</b>  |
| <b>5</b> | <b>EJECUCIÓN</b>              | <b>10</b> |
| 5.1      | Matriz de Resultado           | 10        |
| <b>6</b> | <b>ANÁLISIS FODA</b>          | <b>11</b> |
| <b>7</b> | <b>DICTAMEN</b>               | <b>12</b> |
| <b>8</b> | <b>CONCLUSIONES</b>           | <b>13</b> |

## INTRODUCCIÓN

La seguridad informática se enfoca en la fuga de información que se logra puntualizar como la salida de información de una empresa sin la previa autorización de la misma. Información que para las Empresas es unos de sus Activos más importantes ya que si llega a conocimiento de personas no autorizadas por motivos de descuido o por error del personal encargado de la misma sería de gran problema, sabiendo que es difícil de medir el impacto de la fuga de información ya si este a su vez es proporcionada de manera accidental o incidente malicioso. Por tal motivo a nivel mundial, las empresas y las corporaciones de manera continua implementan nuevas tecnologías para fortalecer la seguridad informática ya que las exigencias del mercado lo requieren para frenar las amenazas y riesgos del sistema informático.

De esta manera se define como causa primordial el descuido del personal respecto a la información reservada de la Empresa. Para abordar esta problemática, es importante nombrar las causas. Una de ellas es la vulnerabilidad informática el cual se puede definir como la debilidad de un sistema de información donde terceras personas violentan de su confidencialidad. Perjuicio significativo que soporta los recursos informáticos afectando su integridad, disponibilidad y confidencialidad, por lo que se recomienda eliminarlas.

La indagación de este problema informático se plasmó por el beneficio de saber que en las últimas décadas se ha aumentado el nivel de riesgo y amenaza, ya que la competencia perfecta es dinámica en las actividades empresariales. Esto ha permitido que la auditoría informática como herramienta que permita evidenciar los aspectos internos y externos que causan la fuga de información en ciertas entidades. Tome medidas de seguridad sobre la información para las Empresas, así mismo la automatización de los recursos controlados que lo conforman y prevenir cualquier tipo de espionaje. Para desarrollar a fondo la investigación desde el punto de vista informático, para ejemplificar con datos estadísticos actualizados respecto al tema propuesto.

Luego de conocer la necesidad de la auditoría Informática tenemos como objetivo determinar cuáles son los factores que inciden en la fuga de información, de esta manera salvaguardar los recursos de la empresa y alcanzar los niveles de seguridad. Para desarrollar la problemática se baso es el enfoque metodológico del libro de Auditoría de los Sistemas Computacionales (Razo, 2002).

## **1 FUNDAMENTACIÓN TEÓRICA**

A nivel mundial precisamente en los años 70 fue desarrollado la auditoría informática por primera vez debido a los determinantes problemas que existía en el desarrollo económica de las empresas de ahí surge la exigencia de realizar la seguridad informática, donde la información no fue confidencial pues para resolver estos problemas se aplicó investigación de las causas y efectos de porque se dio fuga de información aplicando las técnicas de la auditoría (Valencia & Tamayo, 2017).

En consecuencia, los resultados fueron aceptados, comprobados y así mismo desde entonces para medir y controlar los recursos informáticos la auditoría informática es inevitable para la mejora continua de las empresas.

En américa latina, en los últimos 10 años la tecnología ha sido trascendental para el desarrollo económico de las empresas, pero la competencia les obliga mantener seguridad en la información, por ende, el uso de los recursos informático debe ser protegidos y controlable, por cuanto la auditoría se encarga de estudiar y promover cualquier riesgo que puede afectar significativamente la empresa en su conjunto.

En nuestro país, desde el año 2013 ecuador ha fomentado el uso de internet en las empresas y la sistematización de las actividades comerciales (Vargas et al, 2017). Y esto conlleva a que se incrementa el riesgo informático incluso fue aceptada en los convenios internacionales para el uso de las normas de la auditoría, por ende, la auditoría ha formado un papel importante en el desarrollo de las entidades. Puesto que, los recursos informáticos suelen ser vulnerables lo cual conlleva a la fuga de información. Para remediar esta problemática se aplica los procedimientos de la auditoría informática.

### **1.1 Auditoria**

Se entiende por auditoría un conjunto de técnicas y procedimientos sistematizado para entonces le permite evaluar los mecanismos que a su vez se den por inconsistencias, por lo tanto, procederá a implementar normas para el cumplimiento adecuado de las Empresas que lo soliciten (Armijos & Burgos, 2016).

### **1.2 Auditoria Informática**

De acuerdo a (Martinez & Briseida, 2013) la auditoría informática es un proceso sistematizado que tiene por objeto determinar el funcionamiento de los recursos informáticos y proveer el riesgo informático que puede afectar la base de datos de la empresa, también se define como una serie de técnicas y procedimientos que otorga la facilidad a la empresa valorar sus activos controlables.

### **1.3 Seguridad informática**

De acuerdo a una teoría desarrollado por el autor (Miranda et al, 2016) seguridad informática consiste en proteger los recursos informáticos contra cualquier ataque de hacker, virus, spam, y demás programas maliciosos que pueden dañar o perder información.

### **1.4 Tecnología Informática**

Para (Vera & Gil, 2017) la implementación de la tecnología información en las empresas han tenido éxito en el crecimiento de las Finanzas ya que es factor clave para prevenir los ataques y pérdida de información y a su vez obtener una base de información oportuna para el correcto funcionamiento de los sistemas computacionales de la entidad.

### **1.5 Vulnerabilidad**

Es todo lo que incumbe a obtener información o acceso de manera inapropiada, es decir sin la previa consentimiento del personal autorizado. Por tal motivo la vulnerabilidad tiene como finalidad disminuir los riesgos a efecto de la administración de los sistemas operacionales el recurso informático de una empresa determinada afirmó (Pulido et al, 2014).

### **1.6 Fuga de Información**

Según (Cabarique, Salazar, & Quintero, 2015). La fuga de información es un proceso mediante el cual terceras personas llegan a obtener información confidencial de una empresa, por las que se clasifica en factores internos como los personales que laboran dentro de la empresa, por cuanto externos como los clientes, proveedores y la misma competencia. Y para (Amaro, Rodriguez, & Rosalba, 2016) las formas más usuales de fuga de información son el uso de Pendrive, móviles, sitio URL y el libre acceso a lugares restringida de la empresa.

### **1.7 Usuario**

Es toda persona que tiene como objetivo realizar una actividad ya sea esta en lugares públicos o privados, en la cual usa recurso ajeno hasta cierta limitante, con el fin de brindar un servicio utilizando ciertos mecanismos (Hurtado & Fernández, 2015).

### **1.8 ISO 27001**

La norma ISO 27001 constituye una norma Internacional, en la cual se enfoca en sobrellevar de una manera Integra la Información como también a los sistemas que la resuelven, fue diseñada para cubrir los Sistemas de Seguridad de Información, cumpliendo con la función de debilitar o a su vez eliminarlos. De tal manera dar la seguridad a la Empresa para que realice sus actividades de una forma segura (Arcentales & Caycedo, 2017).

## 2 FASE DE LA PLANEACIÓN

### 2.1 Vista Preliminar

La empresa DISROJA Cía. Ltda. Está ubicada en el Cantón Pasaje, fue creada en el año 2010, se dedica a la distribución y comercialización de los productos de consumo masivos. Lo cual demanda de una Auditoría Informática ya que se percató que existe una fuga de información, por lo tanto, se recurre a realizar una visita a cada uno de sus departamentos para constatar las situaciones en que se encuentran, con el Objetivo de Eliminar la causa de la fuga de información.

La empresa está segmentada por cuatro departamentos tales como gerencia, contabilidad, secretaría y logística, cuenta con 4 Computadoras Sony en las cuales lleva sus registros y actividades diarias, mediante un Sistema Operativo Windows 10 que a su vez mantiene sus medidas de protección de Antivirus Actualizados y dispone de un UPS con el propósito de proteger la información, como también instalación de cámaras de seguridad. Bajo un Sistema Contable Sofadcon para sus actividades, por lo que dispone de ocho personas autorizadas para realizar las actividades de trabajo que se rigen a una política sobre las medidas de Seguridad de la Empresa como políticas de uso de Contraseña para los usuarios. El análisis del caso nos lleva a plantear la siguiente interrogación ¿De qué manera afecta a la empresa la fuga de información y cómo influye en los sistemas computacionales? por lo tanto mediante la Auditoría Informática se llegará a conocer la causa de la fuga de Información, que provoca pérdidas Económicas dentro de la Empresa.

### 2.2 Punto A Evaluar

Dentro de los puntos a evaluar para realizar la Auditoría Informática en la Empresa se consideró los siguientes aspectos.

### 2.3 Seguridad Física

- Tiene a su disposición Cuatro Computadoras marca Sony en las cuales lleva sus registros y actividades diarias.
- Está distribuida en cuatro departamentos tales como, Gerencia, Facturación, Contabilidad, Secretaria.
- Tiene un sistema de cámaras dentro y fuera de la empresa para su seguridad.
- Posee de un UPS, con la finalidad de proteger la información y los recursos.
- Consta de una política sobre las Medidas de Seguridad de la Empresa.
- Cuenta con políticas de uso de Contraseña para los usuarios.

## 2.4 Seguridad Lógica

- Dispone de un sistema de protección Antivirus Actualizado.
- Cuenta con un Sistema Operativo Windows 10.
- Para sus Actividades y Obligaciones dispone del Sistema Contable Sofadcon.

## 2.5 Seguridad Personal

- Conocimientos y Experiencia del personal que administra el centro de cómputo.

Plan de Trabajo de la Evaluación de la Empresa Disroja Cía. Ltda.

Por lo tanto, para realizar la Auditoría Informática, se plantió un Plan de Trabajo que él mismo llevará el soporte de sus Actividades a realizar, con el aporte del personal encargado, identificando el tiempo a disponer y de los recursos necesarios mediante la Auditoría Informática que se lo podrá visualizar en las hojas de Anexo #1

## 3 GUÍA DE AUDITORIA

| N | Actividades a Evaluar.   | Procedimiento de la Auditoría.   | Herramientas que serán utilizadas.    |
|---|--|--|---------------------------------------|
|   | Seguridad Física (Hardware)  |  |                                       |
| 1 | Verificación del Hardware  | Se verificará con el encargado de los equipos, la condición, tiempo y uso                          | Manipulación de los Hardware          |
| 2 | Verificar el estado de Almacenamiento del UPS                            | Verificar el Regulador si está apto para su funcionamiento.  | Manipulación del UPS                  |
| 3 | Inspeccionar el cumplimiento de las Políticas del uso de contraseña      | Revisar que no sean visibles ni guardadas en lugares de fácil acceso.                              | Entrevista con el Encargado del Área. |
| 4 | Comprobar el Sistema de cámara de Seguridad dentro y fuera de la Empresa | Verificar el alcance y la correcta ubicación en lugares propicios y revisar el lugar de monitoreo. | Entrevista con el encargado del área  |

|   |   |  |  |
|---|---|--|--|
| 5 | Examinar cada Departamentos dentro de la Empresa                                | Constar si mantiene un aire adecuado para que no sobrecaliente las computadoras, su infraestructura segura de amenazas de agua o fácil acceso              | Observación por parte del auditor,         |
| 6 | Verificar las Políticas de Seguridad de la Empresa                              | Solicitar al encargado el manual de seguridad y comprobar mediante una lectura las medidas de seguridad  | Manual de seguridad                        |
|   | Seguridad Lógica (Software)   |  |  |
| 1 | Revisar el Sistema Contable que utiliza la Empresa (Sofadcon)                   | Manipular el Sistema Sofadcon y sus políticas de privacidad, y su seguimiento por parte de los analistas del sistema                                       | Manipulación del computador.               |
| 2 | Comprobar la Instalación y Actualización del Sistema de Protección de Antivirus | Buscar en el ordenador las licencias de Antivirus y si se encuentran instaladas correctamente y actualizadas para la correcta protección de la información | Ingreso al computador                      |
| 3 | Comprobar el funcionamiento del Sistema Operativo Windows 10.                   | Verificar si el sistema utilizado es acorde a los trabajos que se realizan, y la capacidad es recomendable.  | Análisis al Computador, Sistema Operativo. |
|   | Seguridad Personal  |  |  |
| 1 | Experiencia y conocimiento del personal que administra los centros de cómputo.  | Reunión con el personal para verificar el manual de las políticas de la empresa.   | Entrevista con el personal.                |

#### 4 MATRIZ DE EVALUACIÓN.

Dentro del proceso de la Auditoría Informática tenemos la Matriz de Evaluación, la cual nos detalla los controles a evaluar y a su vez los hallazgos encontrados, que se lo puede revisar en el Anexo #2

## 5 EJECUCIÓN

### 5.1 Matriz de Resultado.

| Punto a Evaluar  | 4-<br>6 | 7-<br>8 | 9-<br>10 | Confianza |
|--|---------|---------|----------|-----------|
| Verificación de los Ordenadores.   |         |         | X        | Alta      |
| Verificación del funcionamiento del Regulador de Voltaje                     |         |         | X        | Alta      |
| Inspección del cumplimiento de las Políticas del uso de contraseñas          | X       |         |          | Baja      |
| Comprobación del Sistema de cámara de Seguridad dentro y fuera de la Empresa |         |         | X        | Alta      |
| Verificación del lugar donde reposa la información de la Empresa.            |         |         | X        | Alta      |
| Medidas de Seguridad Interna que establece la Empresa                        | X       |         |          | Baja      |
| Revisión del Sistema Contable que la Empresa utiliza para sus Actividades    |         |         |          | X         |
| Comprobación de la Actualización del Sistema de Antivirus                    | X       |         |          | Baja      |
| Comprobación del funcionamiento del Sistema Operativo Windows 10             |         |         | X        | Alta      |
| Entrevista con el personal de la Empresa.                                    | X       |         |          | Baja      |



Para la siguiente Evaluación se tomó en consideración los siguientes parámetros, y así determinar cada uno de los factores que provocan la fuga de información, previo a una entrevista a cada personal encargado del área, se logró obtener la siguiente ponderación.

Del 9-10 Alta

Del 7-8 Media

Del 6-4 Baja

- De las 4 computadoras revisadas, todas se encontraban en perfecto estado.
- Luego de revisar el regulador de Voltaje, se verificó que se encontró en perfecto estado.
- No existe integridad en el cuidado de las contraseñas.
- Las cámaras de la empresa, protegen y se encuentran en los lugares adecuados.
- El lugar donde se guarda la información, es segura y libre de amenazas.
- Las medidas de seguridad que plantea la Empresa no se cumplen.
- El sistema contable es de mucha confianza y eficiente para la Empresa.
- El sistema de protección Antivirus, no es seguro.
- El sistema Operativo cumple con las actividades de la Empresa.
- El personal no está capacitado para evitar riesgos y no cumple con las políticas.

## 6 ANÁLISIS FODA

| F  | O  | D  | A                                     |
|--|--|--|---------------------------------------|
| Un correcto funcionamiento del Hardware            | Una Infraestructura adecuada,            | No cumple las políticas de seguridad de la Empresa | Sus contraseñas no son confidenciales |
| Mantiene medidas de protección Antivirus           | Mantiene sistema de vigilancia (cámaras) | Personal con falta de conocimiento                 | Sistemas de Antivirus desactualizados |
| Posee un Sistema contable acorde a sus actividades |  |  |                                       |

## 7 DICTAMEN

Luego de haber realizado el proceso de Auditoría Informática a la Empresa Disroja Cía. Ltda. Se pudo dar a conocer el siguiente Dictamen con Salvedades por la fuga de Información.

Al Gerente de la Empresa DISROJA CÍA. LTDA, se realizó una Auditoría Informática del 15 de diciembre al 15 de enero del 2019, por el motivo de fuga de Información, lo cual la auditoría se basa a pruebas selectivas con evidencias que soporta los planes de trabajo. Considerando que los exámenes demuestran una base sustentable para emitir la opinión.

Se logró detectar que la seguridad de mantener las contraseñas de manera confidencial no se daba, ya que personal no autorizado tiene acceso a ella, contraseñas visibles, logrando así que por desconocimiento generaba riesgo de eliminar información de relevancia de la empresa. Se recomienda mantener una actualización constante de ella y con medidas altas de protección como poseer una combinación de letras mayúsculas, número y signos.

Las medidas de seguridad interna que impone la empresa no se cumple, ya que se observó que el trabajador tiene acceso a los departamentos, Se recomienda que exista dentro de las políticas de la empresa, cierto acceso a personal autorizado, ya que esto conlleva que por falta de conocimiento pueda acceder a un computador y por error eliminar información relevante de la empresa.

Los sistemas de protección de antivirus no se encuentran actualizados, por lo cual existe el riesgo de la fuga de información, ya que es un sistema que detecta y protege la información de cualquier amenaza, y resguarda el deterioro de los archivos, se recomienda utilizar Sistemas de Protección Actuales, (McAfee Antivirus Plus 2018, ESET NOD32 Antivirus 10) y sus actualizaciones constantes.

Cierto personal no tiene conocimiento de la importancia de una fuga de información y del uso exacto de los sistemas, Se recomienda concientizar y disuadir mediante una capacitación sobre el manejo de información y consecuencias laborales y legales.

## 8 CONCLUSIONES.

Luego de haber realizado la Auditoría Informática a la Empresa DISROJA Cía. Ltda. Se pudo verificar varios aspectos, como el incumplimiento de las políticas y medidas del caso establecidas por la empresa, para prevenir la fuga de Información.

- El personal de trabajo no mantiene confidencialidad de su usuario o contraseña, lo cual permite el acceso a personas no autorizadas generando el riesgo de eliminar o enviar información relevante sin su consentimiento, o apoderarse de información que no le pertenece con el fin de lucrarse económicamente, se recomienda contraseñas Segura como la combinación de letras, números, mayúsculas y signos, y para uso personal.
- Dentro de las políticas de seguridad de la empresa, no está establecido la restricción del acceso a personal no autorizado a ciertos departamentos donde se almacén.
- a o guarda información relevante de la empresa, lo cual se pide implementar una Política que restrinja la autorización a ciertos lugares importantes de la empresa, para así poder salvaguardar la información.
- Como medida de protección y amenazas a los programas y sistemas operativos de la empresa, se mantiene instalados programas Antivirus, pero el cual no están acorde a la necesidad de la empresa, ya que esta no mantiene un debido control como es su actualización constante y poder detectar, bloquear y eliminar los virus y otros códigos maliciosos que ponen en riesgo la fuga de Información de la empresa, por terceras personas.
- El conocimiento y preparación del personal es un rol muy importante, ya que por falta de estos recursos se expone a la fuga de información, para poder tomar las medidas necesarias y en el momento oportuno, evitando así la fuga de información.